

REPORT DOCUMENTATION PAGE				Form Approved OMB No. 0704-0188	
<p>The public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing the burden, to Department of Defense, Washington Headquarters Services, Directorate for Information Operations and Reports (0704-0188), 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to any penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.</p> <p><b>PLEASE DO NOT RETURN YOUR FORM TO THE ABOVE ADDRESS.</b></p>					
1. REPORT DATE (DD-MM-YYYY) 26 April 2012		2. REPORT TYPE Master's Thesis		3. DATES COVERED (From - To) 25 July 2011 - 17 June 2012	
4. TITLE AND SUBTITLE Zeroing Biometrics: Collecting Biometrics Before the Shooting Starts				5a. CONTRACT NUMBER	
				5b. GRANT NUMBER	
				5c. PROGRAM ELEMENT NUMBER	
				5d. PROJECT NUMBER	
6. AUTHOR(S) Lt Col Michael R. Green, USAF				5e. TASK NUMBER	
				5f. WORK UNIT NUMBER	
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Joint Forces Staff College Joint Advanced Warfighting School 7800 Hampton BLVD. Norfolk, VA 23511-1702				8. PERFORMING ORGANIZATION REPORT NUMBER	
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)				10. SPONSOR/MONITOR'S ACRONYM(S)	
				11. SPONSOR/MONITOR'S REPORT NUMBER(S)	
12. DISTRIBUTION/AVAILABILITY STATEMENT Approved for public release, distribution is unlimited.					
13. SUPPLEMENTARY NOTES					
14. ABSTRACT The great challenge in defeating an insurgency is the members of an insurgency are often difficult to identify until they are of sufficient strength and choose to challenge openly the established government. Biometrics offers a mechanism that removes an insurgent's anonymity and makes visible their identity, and even their actions, to stabilizing agents (military, police, border guards, and transportation authorities). Analyzing writings of insurgent and counterinsurgent theorists makes it possible to lay out key principles a system like biometrics must influence to be of value. An analysis of these principles shows the Department of Defense's biometric program, as used in Iraq and in Afghanistan, engages most of these principles successfully. However, the key challenge to a successful biometrics program in the future is the need for the collection of biometric information early, preferably before a conflict begins. Targeting biometric collection to areas of strife and against internationally-mobile individuals is a good way to build a sizeable database today. In order to take this next important step the U.S. must provide updated policy and doctrine regarding the collection of biometrics in Phase Zero within enemy geographic combatant command.					
15. SUBJECT TERMS					
16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT  Unclassified Unlimited	18. NUMBER OF PAGES  80	19a. NAME OF RESPONSIBLE PERSON
a. REPORT  Unclassified	b. ABSTRACT  Unclassified	c. THIS PAGE  Unclassified			19b. TELEPHONE NUMBER (Include area code)  757-443-6301

## INSTRUCTIONS FOR COMPLETING SF 298

**1. REPORT DATE.** Full publication date, including day, month, if available. Must cite at least the year and be Year 2000 compliant, e.g. 30-06-1998; xx-06-1998; xx-xx-1998.

**2. REPORT TYPE.** State the type of report, such as final, technical, interim, memorandum, master's thesis, progress, quarterly, research, special, group study, etc.

**3. DATES COVERED.** Indicate the time during which the work was performed and the report was written, e.g., Jun 1997 - Jun 1998; 1-10 Jun 1996; May - Nov 1998; Nov 1998.

**4. TITLE.** Enter title and subtitle with volume number and part number, if applicable. On classified documents, enter the title classification in parentheses.

**5a. CONTRACT NUMBER.** Enter all contract numbers as they appear in the report, e.g. F33615-86-C-5169.

**5b. GRANT NUMBER.** Enter all grant numbers as they appear in the report, e.g. AFOSR-82-1234.

**5c. PROGRAM ELEMENT NUMBER.** Enter all program element numbers as they appear in the report, e.g. 61101A.

**5d. PROJECT NUMBER.** Enter all project numbers as they appear in the report, e.g. 1F665702D1257; ILIR.

**5e. TASK NUMBER.** Enter all task numbers as they appear in the report, e.g. 05; RF0330201; T4112.

**5f. WORK UNIT NUMBER.** Enter all work unit numbers as they appear in the report, e.g. 001; AFAPL30480105.

**6. AUTHOR(S).** Enter name(s) of person(s) responsible for writing the report, performing the research, or credited with the content of the report. The form of entry is the last name, first name, middle initial, and additional qualifiers separated by commas, e.g. Smith, Richard, J, Jr.

**7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES).** Self-explanatory.

**8. PERFORMING ORGANIZATION REPORT NUMBER.** Enter all unique alphanumeric report numbers assigned by the performing organization, e.g. BRL-1234; AFWL-TR-85-4017-Vol-21-PT-2.

**9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES).** Enter the name and address of the organization(s) financially responsible for and monitoring the work.

**10. SPONSOR/MONITOR'S ACRONYM(S).** Enter, if available, e.g. BRL, ARDEC, NADC.

**11. SPONSOR/MONITOR'S REPORT NUMBER(S).** Enter report number as assigned by the sponsoring/monitoring agency, if available, e.g. BRL-TR-829; -215.

**12. DISTRIBUTION/AVAILABILITY STATEMENT.** Use agency-mandated availability statements to indicate the public availability or distribution limitations of the report. If additional limitations/ restrictions or special markings are indicated, follow agency authorization procedures, e.g. RD/FRD, PROPIN, ITAR, etc. Include copyright information.

**13. SUPPLEMENTARY NOTES.** Enter information not included elsewhere such as: prepared in cooperation with; translation of; report supersedes; old edition number, etc.

**14. ABSTRACT.** A brief (approximately 200 words) factual summary of the most significant information.

**15. SUBJECT TERMS.** Key words or phrases identifying major concepts in the report.

**16. SECURITY CLASSIFICATION.** Enter security classification in accordance with security classification regulations, e.g. U, C, S, etc. If this form contains classified information, stamp classification level on the top and bottom of this page.

**17. LIMITATION OF ABSTRACT.** This block must be completed to assign a distribution limitation to the abstract. Enter UU (Unclassified Unlimited) or SAR (Same as Report). An entry in this block is necessary if the abstract is to be limited.

*NATIONAL DEFENSE UNIVERSITY*

*JOINT FORCES STAFF COLLEGE*

**JOINT ADVANCED WARFIGHTING SCHOOL**



**ZEROING BIOMETRICS:**  
**COLLECTING BIOMETRICS BEFORE THE SHOOTING STARTS**

by

**Michael R. Green**

*Lt Col, USAF*

This Page Intentionally Left Blank

**ZEROING BIOMETRICS:**  
**COLLECTING BIOMETRICS BEFORE THE SHOOTING STARTS by**

**Michael R. Green**

***Lt Col, USAF***

A paper submitted to the Faculty of the Joint Advanced Warfighting School in partial satisfaction of the requirements of a Master of Science Degree in Joint Campaign Planning and Strategy. The contents of this paper reflect my own personal views and are not necessarily endorsed by the Joint Forces Staff College or the Department of Defense.

This paper is entirely my own work except as documented in footnotes.

Signature: 

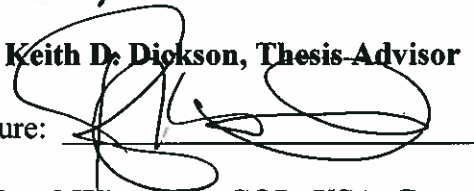
**26 April 2012**

**Thesis Adviser:  
Name**

Signature: 

**Dr. Keith D. Dickson, Thesis Advisor**

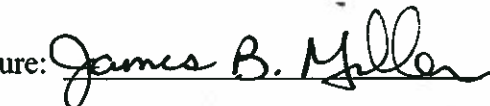
**Approved by:**

Signature: 

**Richard Wiersema, COL, USA, Committee Member**

Signature: 

**Denis P. Doty, Col, USAF, Committee Member**

Signature: 

**James B. Miller, Colonel, USMC  
Director, Joint Advanced Warfighting School**

## **ABSTRACT**

The great challenge in defeating an insurgency is the members of an insurgency are often difficult to identify until they are of sufficient strength and choose to challenge openly the established government. Biometrics offers a mechanism that removes an insurgent's anonymity and makes visible their identity, and even their actions, to stabilizing agents (military, police, border guards, and transportation authorities). Analyzing writings of insurgent and counterinsurgent theorists makes it possible to lay out key principles a system like biometrics must influence to be of value. An analysis of these principles shows the Department of Defense's biometric program, as used in Iraq and in Afghanistan, engages most of these principles successfully. However, the key challenge to a successful biometrics program in the future is the need for the collection of biometric information early, preferably before a conflict begins. Targeting biometric collection to areas of strife and against internationally-mobile individuals is a good way to build a sizeable database today. In order to take this next important step the U.S. must provide updated policy and doctrine regarding the collection of biometrics in Phase Zero within every geographic combatant command.

## **ACKNOWLEDGEMENT**

I acknowledge the Lord, for the determination to see this through and the unexpected way he led a cop into a planning school.

I would like to acknowledge the time and support provided by a great number of the biometrics community for their help in completing this thesis. Specifically, I would like to thank members of the Joint Staff J-8 (Ken Crosby and Jennifer Johnson), members on the OSD staff (Jon Lazar, Ken Kroupa, and Al Miller) as well as SGM Haemmerle, COL Jose Smith, and COL Mark Turner. Any errors contained herein are my own; all astute observations belong to these fine professionals.

I would also like to acknowledge Dr. Keith Dickson for providing the wisdom and guidance to complete this effort.

## **DEDICATION**

This thesis is dedicated to the men and women who have worked to make biometrics a real capability for the U.S. military and the U.S. government. As dollars get tight and “niche” capabilities fade away, may their efforts not be forgotten and the biometrics enterprise continue to produce good fruit.



## TABLE OF CONTENTS

INTRODUCTION .....	1
CHAPTER 1: Theory as a Starting Point: .....	4
Insurgency Theorists .....	4
Mao Tse-tung .....	5
Carlos Marighella .....	8
Al Qaeda .....	10
Counterinsurgent Theorists .....	11
David Galula .....	11
Roger Trinquier .....	13
Sir Robert Thompson .....	14
Key Principles from Theory Review .....	16
CHAPTER 2: Biometrics in Counterinsurgency .....	19
Definition of Biometrics .....	19
Red, Gray, and Blue Biometrics .....	20
The Biometric Trinity .....	21
Biometrics, Forensics and Watchlisting in Counterinsurgency .....	23
Watchlisting .....	24
Types of Biometric Collection .....	24
Fingerprints .....	25
Iris Scan .....	26
Facial Photo .....	27
Biometrics in DoD Today .....	27
CHAPTER 3: Analysis of Biometrics in Two Recent Wars .....	30
Maturing from Defensive to Offensive .....	30
Different Theaters – Different Challenges .....	35
Iraq .....	35
Afghanistan .....	38
Chapter 3 Conclusion .....	40
CHAPTER 4: Phase Zero collection .....	41
Phase Zero Focus for Biometrics .....	41
International Use of Biometrics .....	42

The Risk of Doing Nothing .....	45
Chapter 4: Conclusion .....	46
CHAPTER 5: Biometric Policy: red force collection and sharing .....	48
Biometric Policy on Roles and Responsibilities .....	48
Biometric Policy on Collection and Sharing .....	50
Sharing Biometrics within the U.S. Government (Superseded) .....	50
Sharing Biometrics within the Partner Nations (Superseded) .....	51
Collecting, Storing and Sharing Biometrics in the U.S. and with Partner Nations (New) .....	52
Joint Doctrine on Biometrics .....	53
Joint Publication 3-0 <i>Joint Operations</i> (11 Aug 2011) .....	53
Joint Publication 3-06 <i>Joint Urban Operations</i> (08 Nov 2009) .....	54
Joint Publication 3-07 <i>Stability Operations</i> (29 Sep 2011) .....	54
Joint Publication 3-24 <i>Counterinsurgency Operations</i> (05 Oct 2009) .....	55
Summary of Joint Doctrine .....	55
Presidential Decision Directives .....	55
Presidential Decision Directive/NSC-29 .....	56
Homeland Security Presidential Decision/HSPD-11 .....	56
National Security Presidential Directive 59/Homeland Security Presidential Directive 24 .....	57
Summary and Recommendations .....	59
Identity Management and the DoD Program .....	59
Recommendation for DoD .....	60
Recommendation for the Whole of Government .....	61
Closing the Loop on the Key Principles .....	62
Biometric Collection in Areas with Strife .....	63
Collection Through All Stages of Insurgency .....	63
Biometrics Enables the Mobilization of All Resources .....	64
Biometrics Allows for the Early Defeat of Insurgency .....	64
Biometric Collection is Global .....	65
CONCLUSION .....	66
BIBLIOGRAPHY .....	67
APPENDIX I: General History of Biometrics .....	73
APPENDIX II: Key Biometric Systems .....	77
Department of Defense Automated Biometric Identification System (DoD ABIS) .....	77

Biometric Automated Toolset (BAT) .....	78
Biometric Identification System for Access (BISA).....	78
Handheld Interagency Identity Detection Equipment (HIIDE) .....	79
Secure Electronic Enrollment Kit II (SEEK II) .....	79

This Page Intentionally Left Blank

## INTRODUCTION

*“The problem of destroying enemy armed groups and their supporters therefore consists largely of finding them.”<sup>1</sup>*

*-Frank Kitson*

Defeating an insurgency can be one of the most challenging missions given to any organized force. Countering an insurgency may be the focus of a military campaign or it may be a secondary effort of a more conventional military struggle. In either case, applying all available tools against insurgent vulnerabilities is the best way to ensure success. Biometrics is a tool recently added that has attained a great degree of success in identifying insurgents near U.S. bases as well as within the population. This monograph will examine the application of biometrics to the problem of defeating an insurgency. The thesis of this work is that the United States requires updated policy and doctrine to focus the collection of biometrics in Phase Zero.

In order to be of value to the combatant commander, biometrics must demonstrate effectiveness in counterinsurgency. The first chapter examines the writings of insurgent and counterinsurgent theorists to develop key principles on the nature of insurgency. These key principles highlight in which areas biometrics can have the greatest impact. These principles serve as the consistent scorecard for the effectiveness of biometrics and the Department of Defense’s biometrics program.

Biometrics, like insurgency, is a broad topic. The second chapter discusses important terms regarding the use of biometrics and examines the types of biometrics most commonly used in counterinsurgency. The chapter reviews the history of

---

<sup>1</sup> Frank Kitson, *Low Intensity Operations* (Hamden, Connecticut: Achon Books, 1974), 95.

biometrics within the DoD and concludes with a review of the impact of biometrics on the DoD's counterinsurgency mission.

Chapter 3 examines the application of biometrics in Iraq and Afghanistan. It traces the maturity of the system from a largely defensive operation to one that was later applied with an offensive mindset. It examines the differences between the application of biometrics in Iraq and Afghanistan and identifies the need for the collection of biometric data before the beginning of a conflict.

Chapter 4 argues for the early collection of biometrics during Phase Zero. It also traces the active biometric programs other nations have developed and suggests the U.S. must continue to advance in this field or risk an asymmetric disadvantage in the management of identities and degradation in the ability to screen for suspected terrorists.

Chapter 5 reviews the policy and doctrine documents associated with biometrics within DoD as well as at the Executive Branch level. The chapter concludes that there is additional guidance needed for DoD and the whole of government. Existing policy guidance does not address the importance of collection prior to a conflict and falls short of directing Phase Zero collection.

The recommendations chapter reviews the consistent demand signal from within DoD for updated policy and doctrine, and recommends the completion of a DOTMLPF change recommendation. It also addresses the need for an Executive Order from the President of the United States regarding the focused collection of biometrics by all departments and agencies. The chapter concludes with a review of the key principles unfulfilled by biometrics and suggests improved policy and guidance will remove these deficiencies.

The U.S. employment of biometrics has been effective, but it has also realized limitations. Biometrics is dependent on early collection to be effective. Targeting the collection to areas of strife and internationally-mobile individuals through direct collection and sharing agreements with other biometrically active nations is a good way to build a sizeable database early. In order to take this next important step, updated policy and doctrine regarding the collection of biometrics in Phase Zero of every geographical combatant command is required.

## CHAPTER 1: THEORY AS A STARTING POINT:

*“... the incumbent regime and its military arm present highly vulnerable targets to an enemy who is himself as elusive as the wind.”<sup>1</sup>*

*- Robert Taber*

This chapter reviews key works by insurgent and counterinsurgent theorists in order to develop key principles that serve as the measuring stick for the application of biometrics. It reviews the major elements of insurgency from the perspective of three insurgent writers, beginning with the seminal work of Mao Tse-tung, followed by the writings of Carlos Marighella, and finishes with the more contemporary insurgent writings from Al Qaeda. Following this review is an examination of the work of three classical counterinsurgent theorists. The focus of this chapter is the demonstration of key principles that are common to, and therefore applicable in, the prosecution of future counterinsurgency operations. This manuscript adopts the Joint Staff definition of insurgency found in Joint Publication 3-24, which states, “Insurgency is an internal threat that uses subversion and violence to reach political ends.”<sup>2</sup>

### **Insurgency Theorists**

This section addresses the writing of three insurgent theorists. The purpose of this section is to develop key principles the insurgent may use when attempting to control a government by force or subversion. The section will not cover all aspects of insurgency but it does seek to draw a representation from the rural based philosophy of Mao Tse-tung, to the urban-based philosophy of Carlos Marighella, and the more recent ideology

---

<sup>1</sup> Robert Taber, *The War of the Flea: A Study of Guerrilla Warfare Theory and Practise* (New York: Lyle Stuart, 1965), 19.

<sup>2</sup> U.S. Joint Chiefs of Staff, *Counterinsurgency Operations*, Joint Publication 3-24 (Washington, D.C.: U.S. Joint Chiefs of Staff, 2009), I-1.



of a global insurgent, Al Qaeda. The key principles developed in this section draw heavily from the writings of Mao, and in most cases, other writers have supported or augmented Mao. The seven principles distilled from these writings are:

Insurgent Key Principles
Insurgencies occur in areas with strife
Insurgencies occur in stages
Population is critical to success
Rural and Urban populations are vulnerable
Insurgents are dependent on hiding identity
Supporters bound by ideology not just physical traits
Insurgent support can be global

### Mao Tse-tung

Mao wrote to inspire as much as to instruct on the way a weaker force should engage a stronger force and be victorious. He focused on rural based insurgencies where the population supported insurgents in an area too broad for counterinsurgent forces to occupy. Ultimately, Mao identified three phases to a successful insurgency and articulated clearly the importance of support of the population. In his writing dated May 1938 titled *On Protracted War*, Mao envisioned three stages of conflict:

The first stage covers the period of the enemy's strategic offensive and our strategic defensive. The second will be the period of the enemy's strategic consolidation and our preparation for the counter-offensive. The third stage will be the period of our strategic counter-offensive and the enemy's strategic retreat.<sup>3</sup>

In the first phase, the insurgent focuses on organization of the insurgency, consolidation of resources and support and preservation of the base or safe areas normally located in isolated areas or areas difficult for government forces to occupy. These base areas are key to the insurgency as it is in these areas that training of recruits

---

<sup>3</sup> Mao Tse-tung, *Selected Military Writings of Mao Tse-tung*, (Peking: Foreign Languages Press, 1968), 210-220.

and indoctrination occurs. This is also the phase where active supporters of the insurgency begin to rally support behind the cause and begin to apply pressure to those less receptive to the motivations of the group.<sup>4</sup> The second phase of the insurgency is where the insurgents become undeniable in their acts of terror. If the government was able to turn a blind eye in phase I, they are unable to do so in phase II. Acts of violence increase against weak or isolated police, military or para-military forces with the goal of acquiring arms and ammunition, demonstrating the inability of the government to protect themselves and the people, and gain further support of the population through willful acceptance or coercion.<sup>5</sup> The third and final phase of a Maoist based insurgency involves the final destruction of the enemy. This phase begins when the insurgent forces have grown to a level of strength that they can shed their guerrilla tactics as their primary means of battle and enter into a more conventional style of warfare. Once the insurgency has reached this level of power, they have co-opted large segments of the population and are drawing considerable support.<sup>6</sup> Though this may be the phase of the insurgency where government forces may feel the most comfortable engaging insurgents, a careful insurgent force will not enter this phase until it is certain to have eroded government forces to the point of ineffectiveness.

In addition to arguing for a phased approach to insurgency, Mao also wrote about the importance of political motivation, the value of intelligence, and the critical nature of support of the population. Mao believed in the inexorable link between political goals and the insurgent effort. Without the political objective, the insurgency would lack focus

---

<sup>4</sup> Mao Tse-tung, *On Guerrilla Warfare*, trans. Samule B. Griffith II (Champaign, IL: Universtity of Illinois Press, 2000), 20.

<sup>5</sup> Ibid., 21.

<sup>6</sup> Ibid., 21-22.

and it would lose the support of the people. It was only through the ideological goal that the people would be willing to persevere through the long struggle.<sup>7</sup> On the topic of intelligence, it is important to note the emphasis Mao placed on gathering information about government forces and the strict necessity to deny the same information to the adversary.<sup>8</sup> In phase I and phase II, the insurgent group is operating from a position of weakness relative to government forces and must protect their bases of operation and members with secrecy. Only through a better intelligence network can the insurgent hope to exercise the tactic of, as Mao states:

...seeming to come from the east and attacking from the west; avoid the solid, attack the hollow; attack; withdraw; deliver a lightning blow, seek a lightning decision. When guerrillas engage a stronger enemy, they withdraw, when he advances, harass him when he stops; strike him when he is weary; pursue him when he withdraws.<sup>9</sup>

If successful in gathering intelligence and maintaining secrecy, the insurgent group places the government forces on a lighted stage, watching their every move, predicting their every strike, and ensuring their every effort is wasted.<sup>10</sup>

The last, but equally critical, part of Mao's theory is the ability of the insurgent forces to operate in the rear area of the government forces' defenses. When discussing the relationship of the insurgents to the people he likens it to the same relationship between fish and water.<sup>11</sup> So long as the insurgent remains consistent with the political objectives he has established and these objectives remain in harmony with the population the insurgent finds both support and security within the population. This harmony was so important that Mao established rules for guerrilla fighters to maintain when interacting

---

<sup>7</sup> Mao Tse-tung, *On Guerrilla Warfare*., 43.

<sup>8</sup> Ibid., 22.

<sup>9</sup> Ibid., 46.

<sup>10</sup> Ibid., 93.

<sup>11</sup> Ibid.

with the population, including not stealing from the people and conducting no acts that were selfish or unjust.<sup>12</sup> What is important to grasp is this camouflage is consistent with the insurgent group's continued congruency with the future goals of the population. Those goals may actively support the insurgent group as a result of identifying with the ideological objectives or out of fear and a desire to avoid retribution. In either case, the insurgency finds fertile ground when there is dissonance in some portion of the population and it survives when the population sustains it, by active or passive measures.

### Carlos Marighella

Nations that focus on insurgent bases stemming from rural areas largely use the theories of Mao; however, rural areas are not the only areas that may be inaccessible to government forces. Urban guerrilla warfare is a form of insurgency that has grown in popularity due to failures of a more rural based strategy.<sup>13</sup> A primary text for urban insurgencies are the theories of Carlos Marighella as codified in the "Minimanual of the Urban Guerrilla."

Like Mao, Marighella stresses a need for the urban insurgent to avoid open battle with government forces and instead to draw out government forces to positions of weakness and then attack and disappear before the establishment of a successful counter-offensive. However, unlike Mao, Marighella does not lay out specific phases for the success of the insurgency. What he offers in his manual on urban guerrilla warfare are key concepts that are representative of the urban revolutionary philosophy. First,

---

<sup>12</sup> Mao Tse-tung, *On Guerrilla Warfare*, 92.

<sup>13</sup> Sam Sarkesian, *Revolutionary Guerrilla Warfare* (Chicago: Precedent Publishing, Inc, 1975), 473.

Marighella argues the motivation for insurgency is the desire for political change and this change is in the best interest of the people and for the support of the people.<sup>14</sup> In this way, Marighella and Mao share in the notion of insurgency beginning when there is strife between the people and the government. Where there is a more distinct point of departure is in Marighella's thesis of militarization. He refers to the strategy of "militarization" or the changing of a political crisis into a military situation such that a heavy-handed reaction from the government will alienate the people from government. The objective of militarization is "by inviting repression the urban guerrillas will pave the way for popular revolt."<sup>15</sup>

Second, Marighella sees the exercise of urban violence as a supportive action to a larger strategy that involves rural guerrilla activity. By causing turmoil in the cities, he foresees the confinement of government forces to spaces within the city in order to protect the property of the elite, the businesses, and the financial resources.<sup>16</sup> Thus, the urban insurgent activity paves the way for the gathering of support from the rural population and creates safe areas of operation for the insurgent movement. Third, he holds the same high regard for gathering information on government forces as Mao stressed and speaks with equal vigor about the finding and eliminating of counterinsurgency spies. The security of the insurgent's identity is consistently of paramount importance.

---

<sup>14</sup> Carlos Marighella, "Minimanual of the Urban Guerrilla," in *Revolutionary Guerrilla Warfare*, ed. Sam Sarkesian (Chicago: Precedent Publishing, Inc, 1975), 530.

<sup>15</sup> Robert Moss, "Urban Guerrilla Warfare," in *Revolutionary Guerrilla Warfare*, ed. Sam Sarkesian (Chicago: Precedent Publishing, Inc, 1975), 480.

<sup>16</sup> Marighella, *Minimanual of the Urban Guerrilla*, 528-529.

## Al Qaeda

The third and final review comes from the writings of Al Qaeda. In July 2007, the Congressional Research Service prepared a report analyzing the statements of Osama bin Laden and Al Qaeda from 1994 to 2007. The report serves as an excellent summary of the insurgent philosophy and approach of this group.<sup>17</sup>

To begin with, Al Qaeda recognizes the need for solidarity within the Islamic insurgency as one group united in a defensive Jihad. Osama bin Laden sought to bring together different races, ethnicities, and people of different walks of life under the umbrella of Islam. He sought to wake up what he perceived as the sleeping masses of Islam and return to a preferred time when Sharia law dominated the lives of Muslims under a theocracy referred to as a caliphate. He has appealed to Muslims around the world to be part of this effort and has urged disparate groups representing Sunni and Shia beliefs to avoid violence against one another to preserve a common goal and avoid alienation of moderate Muslims. In a letter between Ayman al-Zawahiri and Abu Musab al-Zarqawi in 2005 addressing violence between Sunni and Shia in Iraq Zawahiri says, “In the absence of this popular support, the Islamic mujahed movement would be crushed in the shadows, far from the masses who are distracted or fearful. . .”<sup>18</sup> In audio and video addresses Al Qaeda has continued to foster a level of cooperation that goes beyond difference within Islam to focus on what is seen as the greater threat from what they call

---

<sup>17</sup> Congressional Research Service Report for Congress, *Al Qaeda: Statements and Evolving Ideology (updated July 9, 2007)*, by Christopher M. Blanchard, <http://www.fas.org/sgp/crs/terror/RL32759.pdf> (accessed October, 17, 2011).

<sup>18</sup> Ayman al-Zawahiri, “Letter in English,” Office of the Director of National Intelligence, [http://www.dni.gov/press\\_releases/ellet\\_in\\_english.pdf](http://www.dni.gov/press_releases/ellet_in_english.pdf) (accessed October 17, 2011).

Jews, Crusaders, and apostate regimes. Al Qaeda, unlike Mao or Marighella, has sought to mobilize insurgents on a global scale.

### **Counterinsurgent Theorists**

While insurgent theorists teach strong lessons, there are also strong lessons provided by their opponents. After surveying three experts in the counterinsurgency field, key principles complementary to the insurgent theorists emerged. Similar to the previous section, this section lists key principles from these authors with a summary of all the key principles at the end of the chapter.

Counterinsurgent Key Principles
Government must mobilize all resources
Insurgencies must be defeated early
Population is crucial to success
Control of population is key
Greatest challenge is identifying insurgents
Large amounts of low level intel necessary
Sustained isolation from insurgents is necessary

### **David Galula**

David Galula is the author of *Counterinsurgency Warfare, Theory and Practice*. Writing in the 1960s, the occurrences of communist-organized insurgencies heavily influenced him, and he wrote about insurgencies occurring in two stages. He divided the stages into a cold stage and a hot stage. In the cold stage, the insurgent group was not conducting violent action and was largely conducting organization and support operations. In the hot stage, insurgents used violence to advance their objectives. In speaking of the hot stage of an insurgency, he outlined two laws of counterinsurgency. The first law is, “The Support of the Population Is as Necessary for the Counterinsurgent

as for the Insurgent.”<sup>19</sup> This law addresses the key challenge for the counterinsurgent, which is the ability to keep an area secure and free from insurgent influence after the departure of counterinsurgent forces. Galula stipulates that counterinsurgency is far too resource intensive for the government to occupy all the terrain all the time and must rely on the population to hold territory after forces have departed. For this reason, he states that the population becomes the objective for the counterinsurgent efforts in much the same way it was the focus of the insurgent.<sup>20</sup> Galula’s second law relates to the first in that the second law states, “Support is gained through an active minority.”<sup>21</sup> In order to secure territory purged of the influence of the insurgent group the population must take an active role in the counterinsurgency effort. Galula states, “In any situation, whatever the cause, there will be an active minority for the cause, a neutral majority, and an active minority against the cause.”<sup>22</sup> Using this premise, he goes on to stipulate that success in a counterinsurgency is not solely the destruction of the insurgent force. A focus of only destroying the forces will result in the recruitment of additional members to the insurgency and a slow but steady shift in the balance of power. Only an elimination of insurgent forces and a permanent isolation of these forces from the population can achieve victory.<sup>23</sup>

In addition to these insightful laws about counterinsurgency, Galula also offers an additional suggestion regarding intelligence in a counterinsurgency. In discussing the execution of an abstract operation to purge insurgents from an area, he emphasizes the need to control the population and develop intelligence. He recommends the use of a

---

<sup>19</sup> David Galula, *Counterinsurgency Warfare* (New York: Frederick A. Praeger, 2005), 74.

<sup>20</sup> *Ibid.*, 74-75.

<sup>21</sup> *Ibid.*, 75.

<sup>22</sup> *Ibid.*, 75-76.

<sup>23</sup> *Ibid.*, 77.



census and the issuing of identification cards as an opportunity to control the population, isolate the insurgents, and develop intelligence necessary to eliminate remnants of the insurgent structure.<sup>24</sup>

### Roger Trinquier

Roger Trinquier is the author of *Modern Warfare, A French View of Counterinsurgency*. He also wrote in the 1960s and his experiences during counterinsurgency operations in Algeria heavily influenced him. Though some overlook Trinquier because of his support for torture when dealing with an insurgency, excepting the torture, his theories have application today. He argued for three principles when fighting guerrillas and stressed the importance of identification of the guerrilla when conducting counterinsurgency operations. Trinquier's three principles for dealing with a guerrilla force are:

To cut the guerrilla off from the population that sustains him; to render guerrilla zones untenable; and to coordinate these actions over a wide area and for long enough so that these steps will yield the desired results.<sup>25</sup>

These three principles are very much in line with the items identified by Galula even though different experiences evoked them. They lend additional support to the conclusions. The principles begin with the displacement of the insurgent forces, followed by the isolation of the insurgent from the population, and conclude with the sustainment of the isolation, which brings the population back under control and eliminates the insurgency. Trinquier also astutely points

---

<sup>24</sup> David Galula, *Counterinsurgency Warfare*, 117-120.

<sup>25</sup> Roger Trinquier, *Modern Warfare* (Westport, Connecticut: Praeger Security International, 2006), 54.

out that before each of these steps can occur the counterinsurgency must identify their target.

Identification of the enemy in modern warfare is extremely difficult. Trinquier points out the boundary between insurgent and supporter of the establishment is often one of ideology.<sup>26</sup> Additionally, the insurgent group is often at an advantage because they start the infiltration of the population long before hostilities begin and before they make their presence known.<sup>27</sup> The solution to this problem is similar to that espoused by Galula and involves the active participation of the population in defense of the government and measures to control the population. Population control begins by establishing a grid system to delineate and segment the area. Once boundaries are established, recommended actions to control and isolate the population from the insurgency include a census, ID cards, fortification of villages, curfews and other measures.<sup>28</sup>

#### Sir Robert Thompson

Sir Robert Thompson authored the book, *Defeating Communist Insurgency, Experiences from Malaya and Vietnam*. His extensive experience in Malaya and Vietnam contributed to his view on counterinsurgency strategy and his approach dominated much of the British way of thinking about

---

<sup>26</sup> Roger Trinquier, *Modern Warfare*, 23.

<sup>27</sup> Ibid., 24.

<sup>28</sup> Ibid., 60-62.

counterinsurgency in the post World War II era.<sup>29</sup> Thompson's writings can be briefly summarized by examining two key points he identified for counterinsurgency operations.

First, the nation should make every effort to defeat the insurgency during the "subversive build-up phase before it enters the guerrilla phase" and if this is not possible it should be defeated as early in the guerrilla phase as possible.<sup>30</sup> Thompson is referring to the stages of insurgency discussed by Mao where the group focuses on organization and the development of support within the population. This is the best time to defeat an insurgency; unfortunately, it is also the least likely time for the governing institution to recognize the existence of the insurgency. Second, Thompson stated "anyone having any responsibility for dealing with an insurgency movement must know his enemy and what that enemy is attempting to do at all stages."<sup>31</sup> In this way, Thompson is arguing for the government to seize the initiative and develop actions in anticipation of the actions of the enemy. He states five clear principles the government must follow: to have a political aim, function within the law, have an overall plan, give priority to defeating the political subversion (instead of simply attacking the physical manifestation of the insurgency), and in the guerrilla phase the government must secure its base areas before moving against the guerrillas.<sup>32</sup> Thompson is arguing for the government to develop a strategy that removes the motivation the insurgents may use to galvanize support from the population and

---

<sup>29</sup> Paul Melshen, "Insurgency Theory ISC7" (lecture, Joint Forces Staff College, Norfolk, VA, September, 2011).

<sup>30</sup> Robert Thompson, *Defeating Communist Insurgency* (London: Chatter and Windus, 1966), 50.

<sup>31</sup> *Ibid.*, 50.

<sup>32</sup> *Ibid.*, 51-57.

secure its own key resources before attempting to engage guerrillas in areas perceived as under guerrilla control.

### **Key Principles from Theory Review**

Key Principles	
From Insurgent Philosophy	From Counterinsurgent Philosophy
Insurgencies occur in areas with strife	Government must mobilize all resources
Insurgencies occur in stages	Insurgencies must be defeated early
Population is critical to success	Population is crucial to success
Rural and Urban populations are vulnerable	Control of population is key
Insurgents are dependent on hiding identity	Greatest challenge is identifying insurgents
Supporters bound by ideology not physical traits	Large amounts of low level intel necessary
Insurgent support can be global	Sustained isolation from insurgents is necessary

What is evident in these key principles is that they are competing but may be viewed as pairings. Victory goes to the side with the best overall execution of the principles. Insurgencies grow in areas where the government fails to meet the needs of the people through decisions limiting the distribution of resources or rights; however, the government must devote resources to defeating the insurgency or risk elimination. The insurgent must grow in strength in secrecy to prevent the government from destroying them at their weakest point. Both sides compete for control of the population in the cities and the country and anonymity is the weapon insurgents use effectively if they are to survive. As the insurgency develops, it draws supporters through its ideology, increasingly from a global audience, and the best defense for the government is the collection of large amounts of low-level information to identify the insurgents and isolate the population from their influence.

At its core, these principles suggest insurgents use anonymity, security and mobility as their key weapons while counterinsurgents focus on achieving visibility, limiting sanctuary, and controlling terrain (physical, human, and ideological). The side

that is most effective at executing these principles is the side most likely to win the conflict. It is not as simple as applying a mathematical equation or establishing discreet measures of effectiveness but the principles do clearly set up a dichotomous relationship. At the heart of the relationship is the question . . . Who are the insurgents? If an insurgency is focused around a core group concerned over ideology, politics, and resource decisions made by the government, then they may represent a limited target population for counterinsurgent forces. However, determining which sub-set of the population is involved in the subversive activity remains a challenge. If the insurgency is drawing from the wider population for material as well as tacit support, the problem magnifies. Likely, the ideological and disaffected youth are used as foot soldiers and less traditional combatants such as women and the elderly are used as facilitators and front line troops. The problem facing the counterinsurgent is how to distinguish the insurgent from within a target population that may include upwards of two-thirds or more of the nation's citizens. The solution may reside within a synergy of biometrics, forensics, and intelligence collection.

Each of these key principle pairings has a biometric component or has the ability to be influence by biometrics. Challenging the anonymity of the insurgent and increasing visibility for the counterinsurgent is a strength of biometrics. The use of biometrics for collection and screening can limit the insurgent's mobility allowing the counterinsurgents to more effectively control ground and limit sanctuary. However, other less obvious principles are linked to biometrics through the collection and application of the science. The recognition that insurgencies begin in areas where there is disagreement with the government and a concentration of disaffected people allows for counterinsurgent forces

to focus their intelligence collection, including biometrics, on these areas. The areas must be recognized to be urban or rural and, while collection of the entire population is desirable, an early collection of a sizeable sample of some segment of the population raises the chances that the counterinsurgent will successfully catalog the information of members early, when the insurgency is weakest.

These key principles will serve as the scorecard for assessing the effective application of biometrics in Iraq and Afghanistan, as well as, the effective application of biometrics in future Phase Zero operations. The following chapters further analyze these principles and introduce biometrics as a technology capable of assisting with counterinsurgency operations.

## CHAPTER 2: BIOMETRICS IN COUNTERINSURGENCY

*“Even after the completion of Overseas Contingency Operations, Biometrics will remain an enduring capability that enables DoD Stakeholders to execute their missions.”<sup>1</sup>*

*-Dr. Thomas Killion, Director Biometrics Identity Management Agency*

Biometrics as a capability has grown remarkably in the past half century. As the technology has become more mainstream, governments and corporations have begun to use biometrics as a means to verify identity and safeguard property. The U.S. has used biometrics extensively on two recent battlefields, in Afghanistan and Iraq. Ultimately, this chapter will show biometrics, though a young technology on the battlefield, is advancing in effectiveness, and can contribute significantly to a counterinsurgency.

### Definition of Biometrics

The term biometrics literally translates to mean “life measurement.”<sup>2</sup> The founder of biometrics was the geneticist Francis Galton, whose contributions to the study of measurement and classification of the human body in 1901 provided significant advances in the classification of fingerprints, leading to the system familiar today. More recent advances in technology have developed the measurement of people into the biometrics used today.<sup>3</sup>

Ben Miller, a leader in the growing biometrics field, coined the following definition in 1987, “Biometric technologies are automated methods of verifying or

---

<sup>1</sup> Dr. Thomas Killion, “National Defense Industrial Association Biometrics Conference Roadmap to Tomorrow” (briefing, to the 2011 National Defense Industrial Association, Arlington, VA, February 23, 2012).

<sup>2</sup> John D. Woodward, Nicholas Orlans and Peter T. Higgins, *Biometrics: Identity Assurance in the Information Age* (Emeryville, CA: McGraw-Hill, 2002), 27.

<sup>3</sup> Whither Biometrics Committee, *Biometric Recognition : Challenges and Opportunities*, eds. Joseph N. Pato and Lynette I. Millett (Washington, DC: National Academies Press, 2010), 16.

recognizing the identity of a living person based on a physical or behavioral characteristic.”<sup>4</sup> Biometrics technology uses measurements taken of an individual and, using an automated process, applies a pre-determined set of parameters to the measurements that are then compared to stored data to retrieve a match. In 2010, the National Research Council defined biometrics as “the automated recognition of individuals based on their behavioral and biological characteristics.”<sup>5</sup> The National Research Council definition uses “recognition” rather than “verification” because there is always a margin of error in any system.<sup>6</sup> Identity based on the parameters of an automated system can be erroneous because the measurements taken can be affected by any number of environmental and temporal factors. However, the basic premise or belief of biometrics is “an individual is more similar to him- or herself over time than to any one else at any time.”<sup>7</sup>

### **Red, Gray, and Blue Biometrics**

Within the Department of Defense, biometrics has three distinct groupings: red, gray, and blue biometrics.<sup>8</sup> Blue biometrics refers to biometrics on trusted members of the Department of Defense, or other partners within the U.S. government. Gray force biometrics refers to those personnel who have been previously vetted and have a need to access a base or be in close proximity to U.S. forces, but are not in a trusted status. Arguably, the first Department of Defense modern biometrics system was the Defense

---

<sup>4</sup> Woodward, *Biometrics*, 27.

<sup>5</sup> Whither Biometrics Committee, 18.

<sup>6</sup> Ibid.

<sup>7</sup> Ibid., 23.

<sup>8</sup> Greg Johnson, “Biometrics Questions & Answers with Greg Johnson,” *Biometrics Bulletin* 2, no. 3 (May/June 2006) [http://www.biometrics.dod.mil/newsletter/issues/2006/may/v2issue3\\_a4.htm](http://www.biometrics.dod.mil/newsletter/issues/2006/may/v2issue3_a4.htm) (accessed November 2011).



Biometric Identification System (DBIDS), conceived in 1995 as a joint venture between United States Forces Korea, the Joint Staff, and the Office of the Secretary of Defense to improve force protection and access control in Korea.<sup>9</sup> DBIDS activated following the terrorist attacks on 9/11 and has remained active in the United States, Korea, and Europe. It is a configurable system designed to control access to installations and sensitive areas.<sup>10</sup> DBIDS largely focuses on blue and gray force identification, controlling access for everyone from military personnel and their dependents to foreign national workers and temporary visitors. DBIDS includes a checking of applicants using various means including comparison against national databases. While a great asset to the Department of Defense, it was not designed to address the challenges associated with the collection and matching of biometrics in the field to find terrorists. Red force biometrics, or biometrics on a population group that represents or may represent in the future a threat to U.S. forces, is the subject of this paper. Red force biometric devices and programs have grown rapidly over the past decade and have become an active part in most ground operations. For an explanation of red force collection systems and national databases see Appendix II.

### **The Biometric Trinity**

No discussion of biometrics is complete without a description of the biometrics trinity and an explanation of how this applies to red force biometrics. The biometrics trinity is a core theme of biometrics when establishing identity and is based on the

---

<sup>9</sup> Office of Management and Budget, Office of Information and Regulatory Affairs, *Defense Biometric Identification System (DBIDS): Attachment 3 Supplemental Information (History)*, Office of Management and Budget, [http://www.reginfo.gov/public/do/PRAViewIC?ref\\_nbr=200812-0704-003&icID=186430](http://www.reginfo.gov/public/do/PRAViewIC?ref_nbr=200812-0704-003&icID=186430) (accessed February, 11, 2012).

<sup>10</sup> U.S. Department of Defense, *DoD Personal Identity Protection (PIP) Program*, DoD Directive 1000.25, (Washington D.C., April 25, 2007).

mantra, “something you have, something you know and something you are.”<sup>11</sup> This is specifically concerned with matching the biometrics of one person for the purpose of recognizing his identity. The phrase *something you have* normally refers to a card, chip, or token that contains a means of cueing the system to the record of the individual. The phrase *something you know* refers to some form of password or other memorized code the person who presents himself for identification passes to the system. The phrase *something you are* refers to the biometric measurements taken and compared to the biometric data in the database. The trinity is normally concerned with identity recognition for blue and gray biometrics. However, during census operations, the identification of residents and the collection of their biometrics, brought together on a biometrically enabled identification card brings two parts of the trinity into play (what you have and what you are) in a one-to one matching situation.

At the core of biometrics, there are two types of matching done in the biometric enterprise. One-to-one matching is largely done in the realm of blue and gray force biometrics where an individual presents himself for verification of their identity. This is most effective in protecting secure areas and denying insurgents access to areas of country or access to population centers where encoded identification cards are used.

Through a token or some other means of connecting the system to their record, the system compares the individual’s biometric traits to the traits on file. If the similarity between the trait presented and the trait on file is close enough to meet the system’s parameters, the system verifies the individual’s identity. The other type of matching is one-to-many matching, which is the act of comparing a presented set of biometric traits

---

<sup>11</sup> Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics, *Report of the Defense Science Board Task Force on Defense Biometrics* (Washington, D.C.: Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics, March 2007), 15-17.

to a stored list of traits. The larger the list of traits the higher the likelihood of a match but the greater the computing power needed and possibly the longer the wait time. One-to-many matching is the more challenging of the two activities but holds the greatest promise for identifying insurgents in the field. It is most often used when comparing biometrics collected on patrol or at incident sites to the collected set of red force biometrics. It can also be used with small data sets of individuals who do not possess a system token. This may occur when comparing the identity of a person requesting entry to a controlled population area against a sub-set of data representing the biometrics of all residents of that area or when verifying identity before issue supplies or medication during a humanitarian operation. From a forensic perspective, one-to-many matching could be the comparison of a latent fingerprint removed from an improvised explosive device (IED) to the entire DoD biometric database.

### **Biometrics, Forensics and Watchlisting in Counterinsurgency**

Biometrics and forensics occur simultaneously on the battlefield; as people and events overlap, the two disciplines support the commander in identifying insurgents. Biometrics and forensics operate together in a counterinsurgency by linking a particular group of people to an event.<sup>12</sup> Biometrics addresses what happens before an event and forensics addresses what needs to take place after an event.<sup>13</sup> The detonation of an IED serves as an example of an event to clarify the relationship. Before the incident, biometrics measures the characteristics of known individuals and enrolls them in a

---

<sup>12</sup> According to Mr. Ken Kroupa, forensics is the “analysis that links persons, places, and things to previous incidents” taken from, Ken Kroupa Sr., “2010 Annual Biometrics Summit: Forensics enabling Biometrics” (briefing, at the 2010 Biometric Consortium Conference, Tampa, FL, September 22, 2010).

<sup>13</sup> COL Mark Turner summarizes the relationship between these two disciplines as follows, “Biometrics maps people on the grid. Forensics tracks them across the grid.” Colonel Mark Turner, phone interview by author, November 9, 2010.

system. After the incident, forensics collects evidence and compares it against biometric data in the database. In the event of a match, the biometrics are flagged in the system through a watchlist to ensure the next encounter with the individual results in action.

### Watchlisting

The watchlist provides units engaged in counterinsurgency the ability to recognize many insurgents and provides leaders with instruction if these individuals are positively identified. Watchlisting is another way of highlighting individuals based on their actions or their associations. When a watchlist is linked to biometric traits, the term biometrically enabled watchlist (BEWL) is used. The U.S. Army through its principal agent, the Biometric Identity Management Agency (BIMA) officially defines the BEWL as “any list of Persons of Interest (POI), with individuals identified by biometric sample instead of by name and the desired/recommended disposition instructions for each individual.”<sup>14</sup> This watchlist has the added benefit of being searchable against multiple databases and supported by forensic efforts at work around the globe. The BEWL is the tool used by commanders when conducting defensive operations, such as screening entrances to bases or controlled population areas, or when conducting offensive operations like raids and directed collections within a specific area.

### Types of Biometric Collection

The Department of Defense uses three primary forms of biometrics collection, often referred to as 10-2-1. This represents ten fingerprints, preferably rolled fingerprint

---

<sup>14</sup> Biometrics Identity Management Agency (BIMA), “Biometrics Glossary,” Version 5.0 (October 2010), under “B,” <http://www.biometrics.dod.mil/Files/Documents/Standards/BioGlossary.pdf> (accessed February 9, 2012).

images, two iris images, and one facial photo. The ten rolled prints, digitally captured but from edge to edge instead of just a flat print, provide maximum utility when comparing against latent prints collected from evidence. The two iris scans enroll the individual for rapid processing or identification at a point of entry or through biometrically enabled passport or visa applications. Lastly, the facial photo provides the most basic recognition features necessary, for identification. Other biometrics available or in use on the battlefield are voice and DNA.<sup>15, 16</sup>

### Fingerprints

Fingerprint identification is done by “using the impressions made by the minute ridge formations or patterns found on the fingertips.”<sup>17</sup> Fingerprints are valuable biometrics on the battlefield for three important reasons. First, the biometric science is well developed and the pattern of fingerprints is unique to every individual.<sup>18</sup> Second, fingerprints are easily and rapidly collected in the field. Technology has greatly improved the quality of the prints collected allowing for low false match rates. Third, forensic specialists can often process latent fingerprints (or prints left behind) and retain them in a database for comparison later.

---

<sup>15</sup>DNA is an excellent source of biometric identification. However, collection and handling of samples in the field is challenging, and the time and cost associated with developing a process for matching is considerably higher than other biometrics options. The upside to DNA, like fingerprints, is its recoverability from a site. The downside is the processing of DNA is considerably more costly than the processing of other biometrics and more time consuming. DNA is unlikely as a form of identification in the field unless the technology advances considerably. As a mode of biometric collection, it certainly has its place on the battlefield but is less functional for the average collector than fingerprints or iris scanning.

<sup>16</sup> The latest in the mobile capture platforms, the Cross Match Technologies Secure Electronic Enrollment Kit II (SEEK II) includes a directional microphone for the capture of a voice sample. This mode of biometric collection is new to the battlefield for the general purpose of biometrics collection and demonstrates the continued advancement of collection platforms.

<sup>17</sup> Report of the Defense Science Board (2007), 28.

<sup>18</sup> Ibid., 25.

## Iris Scan

The iris is a muscle seen as the colored portion of the eye that controls the size of the pupil.<sup>19</sup> Biometric collection involves capturing the random, yet individually unique, pattern of the iris itself.<sup>20</sup> In 1994, Dr. John Daugman developed the algorithms and methods necessary to encode efficiently and compare iris images. The benefits of this form of biometric collection are its speed and extremely low error rates. Once captured, matching of iris images occurs in a matter of milliseconds with very few errors.<sup>21</sup> Dr. Daugman stated:

The mathematics of the iris recognition algorithms make it clear that databases the size of entire nations could be searched in parallel to make a confident identification decision, in about 1 second using parallel banks of inexpensive CPUs, if such large national iris databases ever came to exist.<sup>22</sup>

Iris scanning does have some distinct challenges. Iris scanning technology uses a low level of infrared light to scan the iris and can be subject to environmental interference (such as bright light).<sup>23</sup> Also, a subject can make the collection of an iris scan very difficult simply by closing the eyes. Lastly, there is no forensic link using irises. Unlike fingerprints, forensic retrieval of latent iris images from a crime scene or incident site is not possible because the iris does not make contact with any surface and leaves no impressions. For these reasons, iris scans as a mode of biometric identification,

---

<sup>19</sup> National Science and Technology Council (NSTC), Subcommittee on Biometrics and Identity Management, "Biometrics Foundation Documents," National Science and Technology Council, <http://www.biometrics.gov/documents/biofoundationdocs.pdf> (accessed February 26, 2012).

<sup>20</sup> Report of the Defense Science Board (2007), 28-29.

<sup>21</sup> Ibid.

<sup>22</sup> Woodward, *Biometrics*, 92.

<sup>23</sup> Report of the Defense Science Board (2007), 29.

are more effective where the lighting can be controlled, such as at an entry point to a base/structure, prison, or a border crossing.

### Facial Photo

Facial recognition is the least radical of the modes of biometric collection and may offer the most promise for the future. Facial recognition is the ability to recognize an individual from a photo or other visual representation. It is no different from the process our own brains go through when recognizing someone we know. Although the process of automation has improved in accuracy and speed, unfortunately facial recognition programs are more susceptible to acts of disguise than a human observer.<sup>24</sup> In the field the use of photos remains primarily for human-to-human recognition.

### Biometrics in DoD Today

Biometrics within the Department of Defense existed long before modern forms of biometrics incorporated computer technology. For a general history of biometrics, see Appendix I. The first red force biometric system to enter the Department of Defense's service was the Biometric Automated Toolset (BAT). Following a network vulnerability assessment in Kosovo in 1999, which identified information assurance concerns, the Congress commissioned a study to determine the feasibility of using biometrics within the Department of Defense.<sup>25</sup> BAT quickly became a system for verifying gray forces and flagging debarred (red force) individuals.

---

<sup>24</sup> Report of the Defense Science Board (2007), 25.

<sup>25</sup> Biometrics Identity Management Agency (BIMA), *Biometrics Task Force Annual Report FY 08*, Biometrics Identity Management Agency (Washington, D.C., 2009) <http://www.biometrics.dod.mil/Files/Documents/AnnualReports/fy08.pdf> (accessed February 11, 2012).

A Congressional feasibility study in 1999 determined that “biometric technologies were an emerging capability that would have a significant impact on the DoD and needed to be formalized, centralized, and funded.”<sup>26</sup> In 2000, the Secretary of Defense established the Secretary of the Army as the Executive Agent for biometrics in the Department of Defense. His tasks included the responsibility to coordinate, lead, and consolidate biometrics within the Department. The same year the Biometric Management Office (BMO) was created to serve as the focal point for biometrics for all four branches and received a subordinate unit, the Biometric Fusion Center (BFC) in Clarksburg, West Virginia.<sup>27</sup>

Responsibilities of the BFC included testing commercially available biometric systems for compatibility and use with Department of Defense information systems. In 2004, the BFC became the home of the Department’s Automated Biometric Identification System (ABIS). This was a significant advance in the creation of a large, searchable data set because, up until this time, all the biometric systems in the Department were local systems, with some networking of data using classified lines but working from a limited data set. With the creation of ABIS, the entirety of the biometric collections could now be stored in one location, matched against smaller samples submitted from the field, and compared to other United States government systems run by the Department of Justice and the Department of Homeland Security. In 2006, the organizational structure for biometrics changed as BMO and BFC merged into a single organization known as the Biometrics Task Force (BTF).<sup>28</sup> To enhance support for the warfighter and better represent biometrics to the field, in 2010, the Secretary of the Army officially re-

---

<sup>26</sup> BIMA Annual Report 2008.

<sup>27</sup> Ibid.

<sup>28</sup> Ibid.



designated the BTF as the Biometric Identity Management Agency (BIMA). This re-designation served to make the organization permanent with “the structure and support necessary for biometrics to endure as an enabling capability for the DoD.”<sup>29</sup>

The growing response from the field and the impact of biometrics on operations is visible in a few facts drawn from the BIMA fiscal year 2010 annual report. Submissions to the ABIS database grew from 3,000 a day in FY 09 to on average 6,000 a day in FY 10 with a projected growth up to 35,000 a day in the near future. There were 55,000 latent prints submitted representing a 62 percent increase from FY 09 and more than 3,000 of them were matched to records on file. Thus in FY 10, biometric operations enabled latent print matches on approximately 700 improvised explosive device events and on over 1,300 related watchlist hits.

The success of the biometrics program runs parallel to the size of the biometric database. The first major step was the integration of the collected BAT records from local systems into a single repository. The second major step came in 2007 with the rapid increase in collected biometric signatures through the use of handheld collection devices. The single greatest factor in biometrics is the quantity of the collections.<sup>30</sup> Smart collection through the use of intelligence to pinpoint areas and the recognition of problem areas within a country or hot spots on the globe can improve the collection results. However, the key issue is the fact that there is no substitute for biometric collections in sufficient volume to make watchlisting meaningful and matching through forensics likely.

---

<sup>29</sup> Biometrics Identity Management Agency (BIMA), *BIMA Annual Report FY 10*, Biometrics Identity Management Agency (Washington, D.C., 2011) <http://www.biometrics.dod.mil/Files/Documents/AnnualReports/fy10.pdf> (accessed February 11, 2012).

<sup>30</sup> Large volumes of poorly collected biometrics are of little use; however, the first step must be collection followed by quality control.

### **CHAPTER 3: ANALYSIS OF BIOMETRICS IN TWO RECENT WARS**

*Biometrics is our most effective non-lethal means to protect the Afghan people, protect our soldiers, and separate insurgents from the populace.*

*-SGM Robert Haemmerle*

This section provides an analysis of the use of biometrics in Afghanistan and Iraq. Biometrics matured as a capability from 2001 to today with the introduction of new technology and new ideas. A shift from a defensive mindset to an offensive mindset enhanced by the portability of the technology, made biometrics an effective counterinsurgency tool. The application of this tool was similar in the two conflicts but the existence of an initial set of biometrics and the higher population density in Iraq made the application of biometrics effective earlier despite coalition involvement in Afghanistan pre-dating the Iraq conflict.

#### **Maturing from Defensive to Offensive**

Biometrics has matured in the past decade from a defensive-minded tool to one that is capable of performing offensive-minded actions. Biometrics, as a system for use in contingency operations, began in Kosovo as a means for the U.S. to control access to installations and prevent individuals deemed undesirable from gaining entry to one installation after being barred access to a different installation. In the beginning, employment of biometrics in Afghanistan was done in largely the same way. The Biometric Automated Toolset (BAT) was a force protection tool for controlling access to installations, and for enrollment and tracking of detainee populations. The primary types of biometrics used for access control were fingerprint identification and iris scanning. Identification cards were capable of being produced using the system, but these cards

were not enabled with biometric technology making them little more effective than standard badges produced by a Polaroid camera, cardstock and a laminator. Without the existence of a central repository for biometric data, such as ABIS, which was not operational until 2004, the BAT systems operated as an integrated set of individual systems on the classified network. The systems were not portable and scanning and collection limitations included power and connectivity availability, often placing them at entry control points and key locations interior to the base structure. Biometrics at this stage in its development was largely defensive in nature.

Individuals seeking access to the base would submit to having their biometrics collected but there was not an ability with BAT to move easily into the field to collect biometrics on a target location or at checkpoints removed from the base. The number of individuals requesting access to the installation and the time it took to BAT-check each person further exacerbated the system's limitations. As the war in Iraq began to demonstrate the signs of an insurgency, BAT deployed to this theater of operations with the same type of intent. Biometrics was a force protection tool and flash-pass type badges aided in the circulation control of host-nation and third country nationals operating on base.

As a defensive measure, the use of biometrics was effective but it was not without risk. In 2004 biometrics saw two significant improvements in capability while remaining largely a defensively minded activity. The Automated Biometric Identification System (ABIS) came on line providing the ability to both aggregate the biometric signatures collected by the Department of Defense and to match against the collection for new submissions and biometrics collected by other governmental agencies. This was a

significant improvement to just using local data sets stored within the local BAT servers in Iraq and Afghanistan. This single repository for biometric collection significantly increased the total number of biometric signatures a sample could be compared against and greatly improved the chance of a match. The second major advance came at the cost of 22 lives when in December 2004 a suicide bomber entered a U.S. facility in Mosul Iraq and detonated his device.<sup>1</sup> What followed was a tight six-month development and fielding of an improved force protection system, called Biometric Identification System for Access (BISA), that would collect biometrics of sufficient quality as to be comparable against the ABIS files and FBI biometric files via satellite link. Additionally, these biometric collections could be stored on a biometrically enabled badge to thwart spoofing and counterfeiting. The satellite connectivity raised the timeliness and the probability of a one-to-many match while the biometrically enabled identification cards challenged fraudulent access through one-to-one biometric cueing.

The same year was the first demonstration that biometrics could be more than a defensive tool. In 2004, during United States Marine Corps operations in Ramadi and Faluja, biometrics took a step away from the installations and forward operating bases and became part of the cordon efforts.<sup>2</sup> As Marines used physical barriers to channel vehicle and foot traffic to checkpoints, generators provided power to BAT systems and to iris enrollment devices (Portable Iris Enrollment and Recognition or PIER).<sup>3</sup> The population was enrolled and residents were provided with identification cards to aid in

---

<sup>1</sup> Computer Science Corporation, "Biometrics Identification System for Access," [http://assets1.csc.com/public\\_sector/downloads/0716\\_BISA\\_v6.pdf](http://assets1.csc.com/public_sector/downloads/0716_BISA_v6.pdf) (accessed February 9, 2012).

<sup>2</sup> SGM Haemmerle, phone interview by author, October 18, 2011.

<sup>3</sup> Haemmerle, interview.

the control of civilian traffic in and through the city. Biometrics would, unfortunately, despite innovations such as these, remain defensive-minded through 2006.

What changed in 2007 to move biometrics from a defensively capable system to an offensively minded one? The answer is a change in mindset corresponding to a change in the availability of biometric technology for the conventional force. In January 2007, President George W. Bush announced he was sending an additional 20,000 troops to Iraq as part of an effort to secure the nation and, specifically, the capital of Baghdad.<sup>4</sup> In the same month in Iraq, biometrics went mobile with the introduction of the Handheld Interagency Identity Detection Equipment (HIIDE) devices. These handheld devices considerably increased the range of missions biometrics could support. By roughly March of 2007 each brigade combat team added approximately 200 HIIDEs and 30 BAT kits totaling about 4,000 HIIDES and 1,000 BAT kits in Iraq.<sup>5</sup> As part of Gen Petraeus's plan to secure the city of Baghdad, coalition forces established physical barriers to channel the population while checkpoints screened and enrolled residents much like operations conducted by the Marines in 2004.<sup>6</sup> Multi-National Corps – Iraq (MNC-I) referred to this effort as population control and biometrics were used to monitor the movement of people in, out and through sections of Baghdad.<sup>7</sup>

In addition to population control, the mobile biometrics platforms allowed for increased use and wide spread application of biometrics at checkpoints away from the installation. By removing the tethered power and communications requirements, the

---

<sup>4</sup> George W. Bush, "The New Way Forward in Iraq," (President's Address to the Nation, Washington D.C., January 10, 2007). <http://georgewebush-whitehouse.archives.gov/news/releases/2007/01/20070110-7.html> (accessed February 11, 2012).

<sup>5</sup> Mr. Jon Lazar, phone interview by author, November 2, 2011.

<sup>6</sup> Haemmerle, interview.

<sup>7</sup> Ibid.

mobile devices could be used at a routine checkpoint or rapidly employed at a snap checkpoint. Forces could add these mobile and comparably light systems to mission packages when conducting raids on objectives, conducting searches on suspected improvised explosive device manufacturing locations, or other terrorist hideouts.<sup>8</sup> By targeting the enrollments and the enrollment locations it became possible for coalition forces to gather biometrics on areas known for harboring insurgents or areas with a high incidence of direct and indirect attacks against coalition forces.<sup>9</sup> In the event of an improvised explosive device attack, enrollment of people in the immediate area of the attack was possible. In some cases matches against known or suspected terrorists would occur quickly based on the biometrically enabled watchlist pre-loaded on the device. In other cases it would take time for the forensic material to be processed and the latent evidence compared against the enrollments to determine if anyone at the location had played a role in the attack.<sup>10</sup>

At about the same time this change was occurring in Iraq, the first of 450 HIIDE devices were arriving in Afghanistan.<sup>11</sup> Similarly, forces employed these systems in offensive minded missions not previously possible with the BAT systems alone. Cordoning and searching of areas suspected of containing insurgents now included the use of biometrics. Soldiers and Marines targeted key areas, or areas of a high pattern of insurgent activity, for enrollment with the collections immediately compared to the watchlist information stored in the handheld device. Enrollments were later uploaded to

---

<sup>8</sup> Lazar, interview.

<sup>9</sup> Ibid.

<sup>10</sup> Ibid.

<sup>11</sup> Haemmerle, interview.

the Department of Defense networks and ultimately compared against the sum total of the collections in ABIS.

After 2007, biometrics took on a new direction in Iraq and Afghanistan. While maintaining the defensive capabilities of force protection at the installation by controlling access it was also able to step out in new directions with an offensive mindset enhanced by the portability of the technology. Moving biometrics into operations such as targeted enrollments and raids significantly changed the nature of biometrics on the battlefield.

### **Different Theaters – Different Challenges**

While the technology was the same, the challenges and rate of return of biometrics in Iraq and Afghanistan was different for three key reasons: infrastructure, population density, and the pre-existence of biometric collections. Both theaters were highly dependent on a base of collected material for biometric operations to be successful.

#### **Iraq**

<b>Score Card for Iraq Regarding Use of Biometrics and Key Principles</b>				
		From Insurgent Philosophy		From Counterinsurgent Philosophy
<b>1</b>	<b>√-</b>	Insurgencies occur in areas with strife	<b>√-</b>	Government must mobilize all resources
<b>2</b>	<b>X</b>	Insurgencies occur in stages	<b>X</b>	Insurgencies must be defeated early
<b>3</b>	<b>√</b>	Population is critical to success	<b>√</b>	Population is crucial to success
<b>4</b>	<b>√</b>	Rural and Urban population are vulnerable	<b>√</b>	Control of population is key
<b>5</b>	<b>√</b>	Insurgents are dependent on hiding identity	<b>√</b>	Greatest challenge is identifying insurgents
<b>6</b>	<b>√</b>	Supporters bound by ideology not physical traits	<b>√</b>	Large amounts of low level intel necessary
<b>7</b>	<b>√-</b>	Insurgent support can be global	<b>√</b>	Sustained isolation from insurgents is necessary

Using the scorecard developed in the first chapter as an examination of the effectiveness of biometrics in Iraq is possible. For most key principles and pairings, biometrics demonstrated the ability to aid in the counterinsurgency effort (marked with a check). In some cases biometrics played little role or its performance was severely degraded (marked with an X).

Biometric collection in Iraq got off to a quick start when coalition forces received roughly 300,000 fingerprint cards of Iraqi criminals.<sup>12</sup> These cards served as a base to build the biometric database for the theater and jump-started ABIS. This was possible because of the law enforcement institution that existed in Iraq prior to the invasion. This resulted in un-intended support for the first pairing of key principles. However, the slow recognition of an insurgency and the delay in building sufficient biometric signatures to reach a point where biometrics was operationally significant demonstrate no application of the second pairing of key principles.

As U.S. force collection of biometrics began to take hold using population control techniques and targeted collections using mobile platforms, the U.S. force established a significant repository of biometrics. The greater the base of collection the more likely forensic evidence taken from insurgent activities and locations would successfully identify red force members. The urban nature of the environment enhanced the rapid collection in Iraq and the mobility of the system after 2007 allowed for penetration into less populated areas when needed. Population density was high in the cities and effective population control efforts could net large numbers of collections. Effective use of biometrics to identify insurgents and segregate the population from insurgents was an

---

<sup>12</sup> Haemmerle, interview.



import step toward establishing security in the cities. This application of biometrics in Iraq demonstrates support for the third, fourth, and fifth pairing of key principles.

The improved infrastructure in Iraq allowed for the application of biometrics at internal checkpoints and at international borders. The result was a faster and immediate application of the technology in support of the warfighter by identifying insurgents through the collection of large amounts of biometric data and matching that data to insurgents based on their actions and not their appearance or ancestry. The use of biometrics at the border sought to limit the flow of foreign fighters into the region and cut off the flow of insurgent support (moral and physical). While biometrics was applied to this area, the success of its application was limited by the vastness of the borders and the size of the population coalition forces needed to protect. The key principle pairing of six and seven were demonstrated to varying degrees of success.

Upon analysis of the key principles applied during the conflict in Iraq it is evident that biometrics is an effective tool to aid in combating insurgency. What slowed the application of this capability was the need to build up sufficient biometric signatures to make the matching effective. The dense population and improved infrastructure allowed for the rapid collection of signatures, speeding the application of this counterinsurgency tool.

## Afghanistan

Score Card for Afghanistan Regarding Use of Biometrics and Key Principles				
		From Insurgent Philosophy		From Counterinsurgent Philosophy
1	X	Insurgencies occur in areas with strife	X	Government must mobilize all resources
2	X	Insurgencies occur in stages	X	Insurgencies must be defeated early
3	✓	Population is critical to success	✓	Population is crucial to success
4	X	Rural and Urban population are vulnerable	✓-	Control of population is key
5	✓	Insurgents are dependent on hiding identity	✓	Greatest challenge is identifying insurgents
6	✓	Supporters bound by ideology not physical traits	✓	Large amounts of low level intel necessary
7	X+	Insurgent support can be global	X	Sustained isolation from insurgents is necessary

Coalition forces have been in Afghanistan longer than in Iraq but the maturity of biometric collection grew at roughly the same rate. However, in Afghanistan several challenges delayed the effective application of the technology. Afghanistan lacked the sophistication in law enforcement capability found in Iraq and as such, there was no rapid populating of the biometric database with hard copies of fingerprint cards. The much needed baseline data for comparison of collected biometric signatures had to be built into the database little by little. In September 2009, General Stanley McCrystal challenged his staff to determine the number of collections needed to achieve a tipping point where biometrics collected through both patrols and forensics would begin to return significant matches. This concept was modeled on the success in Iraq and extrapolated to Afghanistan as a percentage of the population. The number was determined to be roughly 1 million collections to achieve the tipping point similar to Iraq.<sup>13</sup> It would be nearly two more years of steady collection in Afghanistan before coalition forces would achieve this level of success. This represents a failure to achieve any reasonable success

<sup>13</sup> Colonal Jose Smith, phone interview by author, October 27, 2011.

regarding the first pairing of key principles. Similarly, despite the early recognition of the insurgency challenges in Afghanistan, the inability of the biometrics program to make gains early demonstrates a weakness regarding the second pairing of principles.

Under General McCrystal's leadership, all doubts were erased about the importance of the population in the counterinsurgency. As coalition forces received the technology to advance collection from the defensive perimeter of the base to a more offensive operation, recognition of the role of biometrics became apparent. Much like Iraq, biometrics was used to identify insurgents and attempt to segregate the insurgents from the people. These efforts demonstrate an effective application of the third and fifth pairing of principles in Afghanistan. However, unlike Iraq, Afghanistan has a largely rural and pastoral population lowering the density of people and reducing the effectiveness of the population collection practices used in Iraq. Further, the continued lack of a reasonable base of collection to compare samples, hindered the biometrics program. In Afghanistan, there is evidence of an inability to apply effectively the lessons from the fourth pairing of key principles.

The transit infrastructure and border crossings in Afghanistan lack much of the development and sophistication found in Iraq. The collection of biometrics at recognized crossings like Spin Boldak in the south remain a focus, but are challenged by poor infrastructure and alternative crossing points. The use of biometrics to identify insurgents regardless of their nationality or affiliation demonstrates support for the sixth pairing but the inability to employ biometrics successfully along the notoriously porous borders of Afghanistan and within the limited transportation infrastructure raises concerns regarding the application of the final key principle pairing.

### **Chapter 3 Conclusion**

During the course of two conflicts, biometrics has matured to a point where it can effectively support counterinsurgency in a majority of the key principles identified. It has moved from a defensive capability to an offensive tool for the identification and capture of insurgents. What is evident from the analysis of its application in Iraq and Afghanistan is that biometrics is heavily dependent on a strong base of collected biometrics for the area. Without this base, forces were required to build the collection pool while conducting other combat and support related activities. Based on the characteristics of the country involved, this may occur over the course of a few years, or it may take a decade to acquire the data needed to apply biometrics effectively. The longer it takes to develop the database the longer the insurgents are likely to maintain their anonymity and grow in influence. Only by beginning the conflict with a robust database can forces be assured of addressing all seven pairs of principles. What the nation needs is the policy and guidance to direct this level of collection.

## CHAPTER 4: PHASE ZERO COLLECTION

*There is no lack of experience data on the disastrous effect of weak intelligence systems in counter-revolutionary warfare.<sup>1</sup>*

*-John J. McCuen*

### Phase Zero Focus for Biometrics

The value of biometrics on the battlefield explains the rapid advancement of biometrics in the Department of Defense. While there has been a distinct evolution from passive uses of biometrics to more offensively-minded operations, biometrics has matured during a time of conflict. However, it is important to look beyond what biometrics has done and understand why it has been successful. Biometrics attempts to achieve identification and remove anonymity. The analysis of insurgent and counterinsurgent theory demonstrated the value of anonymity to the enemy and the fact that long before the first act of violence, stealth is the insurgent's weapon of choice.

For biometrics to continue to mature as a tool for the military, the focus must shift to the application of biometrics as part of the Phase Zero shaping operations of every combatant commander.<sup>2</sup> Phase Zero by definition includes normal military duties such as the collection of biometrics and the sharing of biometrics with partner nations.

Without the existence of large biometric data sets, the existence of robust sharing agreements between the U.S. and other nations is critical. It is largely the DoD's role to make available to the other major users of biometrics (FBI and DHS) biometrics collected outside the borders of the U.S. While both FBI and DHS acquire biometric

---

<sup>1</sup> John J. McCuen, *The Art of Counter-Revolutionary War: The Strategy of Counter-Insurgency* (Harrisburg, Pa: Stackpole Books, 1966), 115.

<sup>2</sup> In the standard construct of a notional operations plan JP 5-0, Joint Operational Planning, identifies six phases. The first phase and the phase that runs continuously before, during and after all operation is Phase Zero. Phase Zero is the shaping operation conducted at the theater and the global level that deters adversaries and solidifies relationships.

signatures on non-U.S. citizens, their ability to gain these signatures is limited to requests for access to the U.S. . . . a defensive mindset. The DoD is the only department capable of targeted collection in hot spots around the world. Coupled with support from the DoS regarding the creation of sharing agreements, the ability to develop a large data set for many areas of the world is a real possibility.

Following the end of the Cold War in 1989 and compounded by the growth of international corporations and free movement and trade zones like the European Union, the borders of nations and the national identity of citizens began to blur. Following the terrorist attacks of 9/11, the perception of terrorist threats to nations highlighted national boundaries and brought back into focus the national identity of travelers.<sup>3</sup> A noted authority on the topic, Benjamin Muller has argued that the application of biometrics has the opportunity to re-establish the solidity of national boundaries and discreetly determine which persons will pass through them.<sup>4</sup> The United States is not the only nation taking a close look at the value of biometric collection.

### **International Use of Biometrics<sup>5</sup>**

The use of biometrics technology has grown in a very short period. The reader should keep in mind the rapid increase in the number of nations using biometrics has far exceeded the number of agreements the DoD has with nations to share the biometrics they collect. While the relationships in the United States as a whole (DoD, DHS, and

---

<sup>3</sup> Benjamin J. Muller, "Risking it all at the Biometric Border: Mobility, Limits, and the Persistence of Securitisation," *Geopolitics* 16, no. 1 (2011): 91-106, <http://ezproxy6.ndu.edu/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=aph&AN=58528598&site=ehost-live&scope=site> (accessed February 29, 2012).

<sup>4</sup> Ibid

<sup>5</sup> A review of the biometric sharing agreements the Department of Defense has with other nations is an important area of study; however, these documents, due to their sensitivity, exceed the scope of this thesis.

FBI) are better together than individually, national caveats often limit the ability to share biometrics received by one department, throughout the U.S. interagency system.

Passports are a common form of identification when moving from country to country. Increasingly, nations are moving to electronic passports also known as e-passports. E-passports meet standards set by the International Civil Aviation Organization (ICAO) to ensure international scanners can easily read them. Of the growing number of nations taking part in this standardization effort, more than 70 nations are including biometrics in their passports.<sup>6</sup> In addition to the standard passport, an embedded radio-frequency identification (RFID) chip in the passport contains biometric and biographic information that the destination end of travel can match. The minimum biometrics to be included in the e-passport is a facial photo for recognition, but many nations are expanding the biometrics included in the passport to fingerprints or iris images. In 2004 the European Union made it mandatory for all e-passports to contain fingerprint images. Of the more than 70 nations using e-passports, 32 require fingerprint images including Venezuela, Nigeria, the Philippines, Bulgaria, and the Czech Republic. Canada is the only nation currently requiring the inclusion of an iris image.<sup>7</sup> Millions of fingerprints are collected routinely as part of normal international travel that happens on a daily basis.

Closely related to passports is the use of biometrics at border crossings. Where passports exist to identify the traveler on the good faith of the issuing nation, other systems are in place to verify identity on behalf of the nation the traveler is entering. Because speed is often important when screening large numbers of travelers, the

---

<sup>6</sup> Dr. Delores M. Etter, "International Biometrics Report" (Report prepared for the Under Secretary of Defense for Policy, Southern Methodist University, Dallas TX, May 3, 2011), 3.

<sup>7</sup> Ibid., 14-15.

biometric of choice is the iris scan. Travelers submit to a scan of their iris and the image is compared to a watchlist to determine if the individual “should be allowed access to the country.”<sup>8</sup> Systems like this are in place in the United Arab Emirates (UAE), the Netherlands, Canada, Germany and the United Kingdom.<sup>9</sup> The UAE boasts iris scans have stopped 70,000 watchlisted individuals from entering the country<sup>10</sup> and since an iris scan takes roughly one second, its popularity is catching on.

Biometrics also has other uses beyond border security. Nations have begun to turn to biometrics as a trusted form of identification for their citizens. Biometrics offers a permanent form of identification that cannot be lost or easily falsified. When conducting a population census there is some support for biometrics saving both time and money while increasing accuracy. In 2010 India launched the first and largest biometric collection effort on its population. As part of this census, India collected facial photos and fingerprints from its 1.2 billion citizens over the age of 15.<sup>11</sup> This census data will serve as the cornerstone of India’s ambitious project to provide each citizen with a unique identification number and ID card linked to facial, fingerprint, and iris biometrics. India is not the only nation using biometrics to track its population. Spain uses fingerprints to enroll and track recipients of healthcare benefits, while Jamaica uses fingerprints to improve the integrity of its voter registration system.

Ultimately, more than 100 nations are collecting biometrics on their citizens and visitors to their country. While many nations are loath to provide biometrics on their citizens unless there is a compelling need, many are willing to share biometrics on

---

<sup>8</sup> Dr. Delores M. Etter, “International Biometrics Report,” 7.

<sup>9</sup> Ibid.

<sup>10</sup> John Daugman, “United Arab Emirates Deployment of Iris Recognition,” University of Cambridge, <http://www.cl.cam.ac.uk/~jgd1000/deployments.html> (accessed February 13, 2012).

<sup>11</sup> Dr. Delores M. Etter, “International Biometrics Report,” 6.



visitors and guests passing through their collection processes. While it may not be possible to collect biometrics on every person directly, it may be possible to gain biometric signatures on much of the world's population, principally the internationally mobile population, through sharing agreements with partner nations.

Working through the collection of foreign visitor biometrics and the verification of citizen's identity through biometrics, nations will soon have the capacity to identify nearly every human on the earth. The nations capable of completing the picture by acquiring the biometric sets of other nations will have a marked advantage in counterinsurgency operations as well as future homeland defense.

### **The Risk of Doing Nothing**

The U.S. has the opportunity to establish the necessary mechanisms to collect and share these signatures in Phase Zero and achieve dominance in the field of identification management. Alternatively, it can pass on this opportunity and allow unfriendly nations the chance to achieve an asymmetric advantage over the U.S. and its allies. If this is to be avoided, partnership with friendly nations to establish sharing agreements must quicken in pace, engagement with neutral nations must begin in earnest, and the U.S. must examine complementary methods for collection of biometrics records contained in hostile nations. Phase Zero is the best time for collection because of the lower cost in lives and the greatest application for the future.

The DoD has three over-simplified options regarding biometrics: maintain the status quo, reduce or eliminate biometrics programs as a cost saver, or increase the emphasis on biometric collection and sharing. The first two options come with varying degrees of the risk of doing nothing and place the military and the United States at risk of

accepting a disadvantage in the global race for the identification of individuals and threat detection.

As biometrics becomes mainstream in partner and adversary nations, the biometric signatures of allied and adversary forces and supporters will increasingly become commodities for trade. Just as the signatures of aircraft and surface vessels represent value to enemy forces, the possession of biometric signatures will increasingly grow in value and the time for collection of these signatures is during Phase Zero. Robust collection of biometrics in one theater has a shaping relationship globally as adversary biometrics, once shared, can aid in the capture of a suspected terrorist in a theater of operations or in the homeland. A robust collection and sharing program can serve as a distinct deterrent to adversaries seeking to enter the U.S. or its facilities anywhere on the planet. Biometrics may not be able to prevent violence from occurring, but with a sufficient database of adversary signatures the likelihood that indications and warning are recognized prior to a significant event are considerably greater than relying on name based searching alone.

#### **Chapter 4: Conclusion**

Biometric collection has demonstrated its value in a counterinsurgency but analysis has also shown that biometrics is far more effective if a sizeable dataset exists before the capability is needed. Preparation of this large dataset is best accomplished through collection and sharing arrangements created during Phase Zero. Other nations are aggressively pursuing biometric collection in order to control both their borders and manage identification of their citizens. If the U.S. does not increase its level of effort regarding the creation of large data sets to secure its borders and identify enemy actors it

runs the risk of falling behind other nations. The U.S. will not be able to stop the aggressive growth of biometrics in other nations but a failure to embrace the value of biometrics could result in an asymmetric disadvantage in this critical area of identity management.

## CHAPTER 5: BIOMETRIC POLICY: RED FORCE COLLECTION AND SHARING

*What do we need to do? Provide the policy and doctrine required to collect biometrics and employ the information/intelligence gained.*

*---Mr. John Boyd Director, Defense Biometrics & Forensics<sup>1</sup>*

The first step in making any systemic change is written guidance providing direction to commanders and justification for acquisitions. The DoD has limited guidance regarding policy for biometrics and even less in the way of joint doctrine. Outside the DoD, there have been efforts to improve the standardization of collection methods in order to enhance interoperability and data sharing but a single overarching executive order addressing collection is missing. What follows is a review of the pertinent directives, doctrine documents, and executive orders regarding biometrics. None effectively addresses the deficiency identified in this study.

### **Biometric Policy on Roles and Responsibilities**

The first DoD directive is DoD Directive 8521.01E, *Department of Defense Biometrics*, dated February 21, 2008. This directive identifies the Principal Staff Assistant (PSA) or the member of DoD responsible for the overall coordination of biometrics to include programs, policy, and interagency coordination, as the Director, Defense Research & Engineering (DDR&E), under the Under Secretary of Defense for Acquisition, Technology, and Logistics (USD (AT&L)).<sup>2</sup> It also designates the Secretary

---

<sup>1</sup> John Boyd., “Looking Back and Moving Forward...DoD Biometrics” (briefing, at the 2011 Biometric Consortium Conference, Tampa, FL, September 27, 2011).

<sup>2</sup> U.S. Department of Defense, *Department of Defense Biometrics*, DoD Directive 8521.01E, (Washington D.C., February 21, 2008).

of the Army as the DoD Executive Agent (EA) for DoD biometrics.<sup>3</sup> Lastly, it designates the flag officers from the Army and Joint Staff to serve as vice-chairs for the PSA when conducting the Biometrics Executive Committee. This directive clearly lays out the roles and responsibilities of the key parts of the biometric structure, but it lacks a corresponding DoD Instruction to describe exactly how these sometimes competing organizations are to work together and advance the biometric enterprise.

The second directive is DoD Directive 1000.25, *DoD Personnel Identity Protection (PIP) Program*, dated July 19, 2004 and certified current as of April 23, 2007. This directive sets policy and establishes responsibilities under the DoD Personnel Identity Protection (PIP) Program. The PIP is DoD's program for:

Addressing threats to the individual personal privacy of its Members, employees, and beneficiaries; establishing a secure and authoritative process for the issuance and use of identity credentials in the Department of Defense; and ensuring that DoD benefits and access to DoD physical and logical assets are granted based on authenticated and secure identity information.<sup>4</sup>

The PIP refers to the larger effort to protect identities within the Department and where this directive touches on the subject of this thesis is through its focus on the identification of access control systems and steps necessary to ensure the protection of collected identities. It is more closely associated with concerns regarding privacy of blue force biometrics and plays little role in this discussion.

---

<sup>3</sup> DoD Directive 8521.01E.

<sup>4</sup> U.S. Department of Defense, *DoD Personal Identity Protection (PIP) Program*, DoD Directive 1000.25, (Washington D.C., April 25, 2007).

## **Biometric Policy on Collection and Sharing**

The memorandum on collection and sharing is a brand new document issued by the Deputy Secretary of Defense late in the development of this thesis. The memorandum validates many of the arguments made throughout this manuscript but is less forceful in its direction to CCMDs regarding the early collection of biometrics. What follows is a review of the two memoranda that served in this efforts initial review of DoD policy as well as an assessment of the new memorandum issued in January 2012.

### **Sharing Biometrics within the U.S. Government (Superseded)**

The memorandum titled *Sharing of DoD Biometric Data and Associated UNCLASSIFIED Information from Non-U.S. Persons with Interagency Entities* dated January 10, 2007 addressed the need to share biometric data within the U.S. government for the purposes of national security. The memorandum stated the need for written requests for the sharing of biometric data possessed by the DoD.<sup>5</sup> This requirement likely referred to organizations in the government that did not already have an agreement with the DoD. The DoD has had a long-standing agreement with the FBI for the sharing of biometric information but, until recently, did not have such an agreement with the Department of Homeland Security (DHS). The GAO highlighted this lack of an agreement in a report titled, *DOD Can Better Conform to Standards and Share Biometric Information with Federal Agencies*, released May 2, 2011. In the report, the GAO chastised the DoD for not completing a sharing agreement with DHS. While the GAO report was still in draft, DoD moved up its timetable for the completion of this agreement

---

<sup>5</sup> U.S. Department of Defense, *Sharing of DoD Biometric Data and Associated UNCLASSIFIED Information from Non-U.S. Persons with Interagency Entities*, Deputy Secretary of Defense Memorandum, (Washington D.C., January 10., 2007).

and was able to sign an agreement with DHS on March 3, 2011.<sup>6</sup> The progress of this agreement notwithstanding, the policy memorandum for DoD sharing of biometrics with other U.S. agencies was outdated and a fresh document, preferably in the form of a formal directive, was needed.

#### Sharing Biometrics within the Partner Nations (Superseded)

The fourth policy document, also dated 10 January 2007, was titled, *Sharing of Biometric Data and Associated Information from Non-U.S. Persons with Coalition Forces and Allies*. The memorandum briefly and accurately stated U.S. forces were engaged in the collection of biometric data as well as partner nations and stressed the need for DoD to establish sharing agreements where biometrics collected by one country could further the force protection of all the nations involved. This sharing excluded any collection on U.S. persons but recognized some nations will have access to data other nations may not and only by sharing biometric signatures on individuals could nations achieve the level of awareness needed.<sup>7</sup> Unfortunately, this memo had three significant weaknesses. First, the memo was four years old and did not take into account many advances in biometrics. The memorandum would better serve the community if incorporated into a directive or instruction that maintained its authority over time and was subject to a review process for update and revision. Second, the memo heavily focused on the conflicts in Iraq and Afghanistan. The memorandum did include a reference to

---

<sup>6</sup> U.S. Government Accounting Office, *Defense Biometrics: DOD Can Better Conform to Standards and Share Biometric Information with Federal Agencies*, Report, GAO-11-276, (Washington D.C., March 2011).

<sup>7</sup> U.S. Department of Defense, *Sharing of Biometric Data and Associated Information from Non-U.S. Persons with Coalition Forces and Allies*, Deputy Secretary of Defense Memorandum, (Washington D.C., January 10, 2007).

“other missions related to national security” but the age of the memo and its specific focus on operations IRAQI FREEDOM and ENDURING FREEDOM made it a backward focused policy as opposed to forward looking one. Third, the memorandum was essentially about sharing and assumed collection was occurring at a pace commensurate with the need for national security. It did not direct the collection of biometrics or the inclusion of biometrics in plans produced by the combatant commanders. This memorandum served to address a need for sharing during a time of conflict but did not have the vision to address future collection needs of U.S. forces.

#### Collecting, Storing and Sharing Biometrics in the U.S. and with Partner Nations (New)

On January 13, 2012 the Deputy Secretary of Defense signed a new policy memorandum titled, “*Authority to Collect, Store, and Share Biometric Information of Non-U.S. Persons with U.S. Government Entities and Partner Nations.*” This policy memo removes many of the weaknesses identified above but it does not go far enough toward addressing early collection of biometrics. Unfortunately, however, this new memorandum, is For Official Use Only and cannot be addressed in detail in this thesis.

With the new date, the memorandum removes the concern of the policy being outdated. Further, the memorandum does not focus on current named operations but addresses a wide range of military operations. Finally, this memo addresses the topic of biometric collection taking a step beyond its predecessor document that focused primarily on sharing.<sup>8</sup>

---

<sup>8</sup> U.S. Department of Defense, *Authority to Collect, Store, and Share Biometric Information of Non-U.S. Persons with U.S. Government Entities and Partner Nations*, Deputy Secretary of Defense Memorandum, (Washington D.C., January 13, 2012).



Where the memorandum falls short is in two areas. First, it is a policy memorandum and is at risk of going out of date much like previous memoranda. The guidance in this policy document serves DoD better in the form of a DoD directive or instruction. Second, this document uses words like “authorized” and “encourage to” and fails to achieve the level of direction needed to ensure CCMDs initiate collection of biometrics and biometric sharing agreements such that biometric signatures exist in sufficient numbers to be of value immediately on initiation of hostilities in any given geographical region.

### **Joint Doctrine on Biometrics**

A complete review of Joint Publications shows biometrics is in eight separate publications. The majority of these references are within the operational series but there is one reference in the main joint intelligence publication. All the publications do little to provide guidance to the commander regarding the collection of biometrics. A review of the pertinent publications follows.

#### *Joint Publication 3-0 Joint Operations (11 Aug 2011)*

This core publication to operational doctrine mentions biometrics but does so only as an example of a technology used when identifying terrorists. The reference is fleeting and specially addresses working with law enforcement by using facial recognition to identify terrorists and their human networks.<sup>9</sup> It provides little beyond a cursory treatment of biometrics and its focus on facial recognition overstates the value of this developing technology.

---

<sup>9</sup> U.S. Joint Chiefs of Staff, *Joint Operations*, Joint Publication 3-0 (Washington, D.C.: U.S. Joint Chiefs of Staff, August 11, 2011), V-3.

Joint Publication 3-06 *Joint Urban Operations* (08 Nov 2009)

Joint doctrine on urban operations is almost equally limited in its discussion as its parent document. JP 3-06 addresses biometrics from the perspective of sustainment, listing biometric equipment as an item for consideration in an urban environment in the same sentence as kneepads and batteries.<sup>10</sup> Despite its release in 2009, the document fails to address any of the lessons learned in Iraq regarding the value of biometrics when conducting operations in a densely populated area.

Joint Publication 3-07 *Stability Operations* (29 Sep 2011)

Joint doctrine on stability operations offers one of the best discussions of biometrics in doctrine today but it is also limited to just a few sentences in two sections of the publication. In Chapter III on Stability Operations Functions, when discussing the contribution of military forces, the publication accurately identifies the role of biometrics in identifying individuals, managing the local population, controlling access to locations and linking identities to forensic evidence.<sup>11</sup> In addition, in Chapter II, when discussing stability operations design and planning, doctrine addresses the importance of biometrics as a population control measure when physically securing the population.<sup>12</sup> What doctrine does not do is stress the importance of collecting biometrics as early as possible. When discussing military involvement in stability operations the time for collecting biometrics is long past due. Biometrics is most effective when available before or as soon as forces reach the area of operations.

---

<sup>10</sup> U.S. Joint Chiefs of Staff, *Joint Urban Operations*, Joint Publication 3-06 (Washington, D.C.: U.S. Joint Chiefs of Staff, November 8, 2009), IV-40.

<sup>11</sup> U.S. Joint Chiefs of Staff, *Stability Operations*, Joint Publication 3-07 (Washington, D.C.: U.S. Joint Chiefs of Staff, September 29, 2011), III-10

<sup>12</sup> *Ibid.*, II-10.

### Joint Publication 3-24 *Counterinsurgency Operations* (05 Oct 2009)

It is in this publication where the best reference to the use of biometrics should reside but it does not. Unfortunately, this doctrine document limits its discussion of biometrics to a discussion of counterintelligence and the need to verify sources. It states, “Background screenings should include collection of personal and biometric data and a search through available reporting databases to determine whether the person is an insurgent.”<sup>13</sup> While this is an important use of biometrics, it is regrettable that this publication does not have more of a discussion to guide the use of biometrics for the Joint Force when conducting counterinsurgency operations.

### **Summary of Joint Doctrine**

While the term biometrics has begun to percolate into joint doctrine publications, they do not adequately express its value as an enabler to U.S. missions when conducting counterinsurgency and stability operations. Routine reviews have sprinkled biometrics through a few publications but there is no concentrated effort to provide guidance to the joint force on the usefulness of biometrics and the means to employ this capability.

### **Presidential Decision Directives**

The issue facing the U.S. is not limited to the DoD. Policy and direction must also include all of the departments who collect biometrics. The best means to achieve integration between various departments within the Executive Branch is through some

---

<sup>13</sup> U.S. Joint Chiefs of Staff, *Counterinsurgency Operations*, Joint Publication 3-24 (Washington, D.C.: U.S. Joint Chiefs of Staff, October 5, 2009), V-6.

form of executive order.<sup>14</sup> For an understanding of the biometric relationship between DoD, DHS, and DoJ, see appendix II. Presidents have used various forms of this authority to communicate their desires and set policy for the U.S. On the topic of biometrics there have been five executive order variations impacting the biometric enterprise. Of those five, three have enough relevance for discussion.

#### Presidential Decision Directive/NSC-29

Presidential Decision Directive/NSC-29, issued by President William Clinton established the Security Policy Board. The Facilities Protection Board, a sub-committee of the Security Policy Board, in turn, established the Biometric Consortium. This Consortium was chartered in 1995 to promote the science of biometrics, create collection and transmission standards for biometrics, and improve information exchange between the government and private entities.<sup>15</sup> While this Consortium sponsors annual conferences and brings together stakeholders from the government, private industry, and academia it is not chartered with ensuring the development of robust biometric data sets or managing collection of biometrics outside the U.S.

#### Homeland Security Presidential Decision/HSPD-11

Homeland Security Presidential Decision/HSPD-11 was issued in 2004 for the purpose of improving the detection and interdiction of suspected terrorists. The Decision sought to improve terrorist-related screening in order to improve homeland defense. It

---

<sup>14</sup> Congressional Research Service Report for Congress, *Presidential Directives: Background and Overview* (updated April 23, 2007), by Harold C. Relyea. <http://www.fas.org/irp/crs/98-611.pdf> (accessed April 4, 2012).

<sup>15</sup> Biometric Consortium, “Charter,” (December 7, 1995), <http://www.biometrics.org/html/REPORTS/CTST96/> (accessed April 4, 2012).

directed DHS to return with reports regarding the improvement of such screenings and the sharing of information between agencies.<sup>16</sup> As it relates to biometrics, the essence of the directive is the ability to recognize a terrorist when their information is presented at one of the biometric collection points controlled by the U.S. For example, it seeks to improve the ability of border screeners in the U.S. and DoS employees screening visa application outside the U.S. to identify terrorists. While it is a necessary step for homeland defense, it is largely defensive in mindset. It is akin to the early development of DoD military practices with biometric collection where screeners waited for individuals to present themselves for screening before collection occurred. The Directive does not provide any increase direction or authority regarding the collection of biometrics.

National Security Presidential Directive 59/Homeland Security Presidential Directive 24

National Security Presidential Directive 59/Homeland Security Presidential Directive 24 was issued in June 2008.<sup>17</sup> The directive “establishes a framework to ensure that Federal executive departments and agencies use mutually compatible methods and procedures in the collection, storage, use, analysis, and sharing of biometric and associated biographic and contextual information of individuals.”<sup>18</sup> This directive, like HSPD-11, seeks to improve the compatibility and sharing capabilities of the executive

---

<sup>16</sup>President, Homeland Security Presidential Directive/HSPD-11, “Comprehensive Terrorist-Related Screening Procedures,” Public Papers of the Presidents of the United States: George W. Bush (2004, Book II), p. 1763 1765, <http://www.gpo.gov/fdsys/pkg/PPP-2004-book2/pdf/PPP-2004-book2-doc-pg1763.pdf> (accessed April 4, 2012).

<sup>17</sup> President, National Security Presidential Directive/NSPD-59 and Homeland Security Presidential Directive/HSPD-24, “Biometrics for Identification and Screening to Enhance National Security,” Weekly Compilation of Presidential Documents Volume 44, Issue 22 (June 9, 2008), <http://www.gpo.gov/fdsys/pkg/WCPD-2008-06-09/pdf/WCPD-2008-06-09-Pg788-2.pdf> (accessed April 4, 2012).

<sup>18</sup> Ibid.

departments in an effort to identify terrorists when they are encountered. The Directive does not provide direction to the departments to focus or increase collection for the U.S. biometric database, either through direct or indirect means. There exists a common theme from the creation of the Biometric Consortium as a derivative of PDD-29, through HSPD-11 and NSPD-59/HSPD-24 for improved standardization and sharing within U.S. departments. However, none of these PDs get to the challenge presented by this thesis, the need to develop U.S. biometric data during Phase Zero within regions likely to generate individuals of specific threat to U.S. safety and security.

## SUMMARY AND RECOMMENDATIONS

Biometrics, as a capability, has been demonstrated effective. What the capability lacks is direction both within the Department of Defense and from the head of the Executive Branch. Within the DoD the solution is a doctrine, organization, training, materiel, leadership and education, personnel and facilities (DOTMLPF) Change Recommendation (DCR). For the whole of government the solution is an Executive Order in the form of a National Security Presidential Directive regarding the focused collection of biometrics.

### Identity Management and the DoD Program

In September 2008, U.S. Joint Forces Command completed an Initial Capabilities Document (ICD) titled *Biometrics in Support of Identity Management*. The document was built on a previous Joint Capabilities Document (JCD) bearing the same title and addressed potential ways to fill capability gaps highlighted in the JCD.<sup>1</sup> The ICD has served as the seminal work for the DoD biometrics program.<sup>2</sup> Two capability development documents (CDDs) were spawned from this ICD but, though it was strongly recommended by the ICD, no DCR has been produced. The purpose of a DCR is to address those non-material items inhibiting the mission and the next section will show non-material items continue to remain a challenge.

---

<sup>1</sup> U.S. Joint Forces Command, "Initial Capabilities Document (ICD): Biometrics in Support of Identity Management," Washington D.C. (September 2, 2008).

<sup>2</sup> In the Joint Capabilities Integration Development System (JCIDS) process used today, the ICD is the first major program document reviewed by the Joint Requirements Oversight Committee (JROC) and is normally followed by a Capabilities Development Document (CDD) and/or a doctrine, organization, training, materiel, leadership and education, personnel and facilities (DOTMLPF) Change Recommendations (DCR). A CDD puts a program on a path to a material solution while a DCR recommends largely non-material changes to mitigate gaps.

## **Recommendation for DoD**

A Joint Staff Action Package (JSAP) was issued by the Joint Staff in 2011 to gauge the need within the CCMDs and Services regarding biometrics. The topic was briefed to the Biometric Executive Committee on 23 Jun 2011 with responses incorporated from CENTCOM, SOCOM, SOUTHCOM, EUCOM, NORTHCOM, AFRICOM and the four services.<sup>3</sup> The Joint Staff asked the respondents to identify the top five priorities the community should focus on in the near future. Some respondents identified five areas while others identified more. Grouped together by type; the “top 9” priorities were established. Of the nine categories, the most sought after area for improvement was policy and doctrine.<sup>4</sup> For example, the Navy listed the number one priority as policy guidance directing the use of biometrics and the number two priority as updating existing DoD directives.<sup>5</sup> The Air Force listed policy as the number two priority and the Marine Corps listed it as number five.<sup>6</sup> Likewise, CCMDs weighed in heavily on the need for updated policy and doctrine regarding biometrics. Reminiscent of the DCRs recommended by the ICD in 2008, the community sent a strong signal for non-material change to the biometrics program.

The first recommendation is for the Army to complete a DCR, specifically focused on the update of policy and doctrine regarding the collection of biometrics. Though the Army serves as the Executive Agent for biometrics there is nothing precluding the Services or the Joint Staff from completing the DCR if interested. The DCR would serve to provide guidance and advance biometrics in a number of key areas.

---

<sup>3</sup> U.S. Joint Chiefs of Staff, “Stakeholder Priorities” (briefing, Biometrics Executive Committee, Washington D.C., June 23, 2011).

<sup>4</sup> Ibid.

<sup>5</sup> Department of the Navy response to Joint Staff Action Package J-8A 00077-11

<sup>6</sup> Department of the Air Force and Headquarters United States Marine Corps MC responses to Joint Staff Action Package J-8A 00077-11.



This updated guidance placing the focus of the collection effort on Phase Zero would greatly improve the effectiveness of biometrics in the next conflict.

### **Recommendation for the Whole of Government**

Before the creation of the Biometric Consortium, users of biometrics struggled with a coordinated approach to biometrics. Executive orders have sought to standardize the collection and storage methods in order to improve the sharing of data and enhance the detection of terrorists. The slowness of this process is indicated by the multiple Executive Orders addressing the same concern; however, none of the orders address the problem highlighted in the Iraq and Afghanistan review. Without a robust set of data, the ability to match is severely degraded. Certainly, the ability to share within the different departments addresses part of this issue; however, it does not get to the larger issue of focused collection in Phase Zero through direct collection by the U.S. or the sharing of information already collected by other biometrically involved nations.

The second recommendation is an executive order addressing the need for biometric collection during Phase Zero. A National Security Presidential Directive placing the Department of Defense in charge of organizing the collection priorities would be valuable. Through the support of the Department of State, the number of sharing agreements could be increased while the U.S., either directly or by proxy, could collect biometrics in regions with suspected insurgent activity. Such a directive would provide support for the military to help fund the development of biometric programs in struggling nations where insurgency is a concern. Likewise, humanitarian assistance missions could contain a second military objective of biometric collection. Finally, it would provide

support for opportunities to acquire biometric signatures using international criminal files and the sharing of biometrics on non-citizen travelers using border crossing and airports.

### **Closing the Loop on the Key Principles**

	Key Principles		
	From Insurgent Philosophy		From Counterinsurgent Philosophy
X	Insurgencies occur in areas with strife	X	Government must mobilize all resources
X	Insurgencies occur in stages	X	Insurgencies must be defeated early
✓	Population is critical to success	✓	Population is crucial to success
✓	Rural and Urban population are vulnerable	✓	Control of population is key
✓	Insurgents are dependent on hiding identity	✓	Greatest challenge is identifying insurgents
✓	Supporters bound by ideology not physical traits	✓	Large amounts of low level intel necessary
X	Insurgent support can be global	✓	Sustained isolation from insurgents is necessary

Biometrics has demonstrated its ability to support an interagency counterinsurgency effort on the majority of these key principles but it falls short on five, not for lack of ability, but for lack of direction. Re-focusing biometrics on a Phase Zero collection strategy that emphasizes the benefits of collection before conflict prepares the commander for the prosecution of the effort in follow-on phases if necessary. Only through this re-focus, combined with refinement through a DCR to focus the efforts of the DoD and an Executive Order to focus the efforts of the interagency, can biometrics improve its ability to support counterinsurgency.

## Biometric Collection in Areas with Strife

Biometrics has, up to this point, been largely about the collection of signatures in the areas of Afghanistan and Iraq. The world is full of areas of strife manifested by civil unrest, weak governments, famine, and poverty. In these areas the U.S. or partner nations are often present. These areas represent the most likely location for future conflict involving insurgents or serve as the most probable breeding ground for insurgents. By targeting collection in these areas as part of other duties performed, there is a real opportunity to develop a database of biometric identities that will be of use in the future. Although biometrics can be collected at any time, waiting for a location to manifest into an emergency may be too late to begin collection based on the lessons of theory and history.

## Collection Through All Stages of Insurgency

Insurgencies happen in stages but an insurgency is not normally visible as a threat until it has passed beyond the first stage. However, insurgencies are prone to begin in places where there is division within the population or between the population and the government. If the U.S. adopts a strategy to collect biometrics in areas with visible strife or to empower cooperative governments to collect in these areas, there are two very likely results. First, the likelihood that potential insurgents will think carefully about threatening violence if their anonymity is in jeopardy is high. Second, those that do take up violence will have a far greater chance of being identified and the tipping point, where biometrics and forensics provide a key enabling function, will happen quickly.

## Biometrics Enables the Mobilization of All Resources

A key challenge of dismantling an insurgency is the intensity of the resources required to protect the population because there are no clear lines of battle and the insurgent can be anywhere. With the use of biometrics, the ability to identify the insurgent becomes possible and measures to control the population and protect it from the physical violence and ideological influence of the insurgents become manageable. With the ability to identify the insurgents, the resources of the nation can be mobilized in a concerted effort to defeat the threat instead of disparate efforts each seeking to find the threat. This does not diminish the intensity of counterinsurgency operations; however, it does offer the chance to avoid waste and reduces the likelihood that efforts taken by the government will further alienate their population.

## Biometrics Allows for the Early Defeat of Insurgency

The earlier an insurgency can be defeated the better the chances of success. Biometrics allows for the identification of insurgents seeking to infiltrate a nation in order to export radical ideology or to assist indigenous groups. The recognition of increased levels of suspect visitors to areas is a key indicator that early levels of insurgency planning are in progress. Biometrics can serve as a key indicator to allow a government to address policy concerns before they erupt in the streets or, failing reconciliation, identify and eliminate threats to the established order.

## Biometric Collection is Global

As globalization continues to bring the world closer together physically and through the internet there must be the recognition that problems that begin in one area are spreading more rapidly beyond the border region of the nation originally involved. The ungoverned spaces of Afghanistan gave rise to threats to the United States and other areas of the world offer similar threats. By collection in one area against a potential threat, biometrics actually provides value in the prosecution of counterinsurgency in other areas. As radical ideology and violence is a global phenomenon, the collection of biometrics can and must be a global effort to be effective.

## **CONCLUSION**

Biometrics is proven on the battlefield in a counterinsurgency environment. In Iraq, the existence of an initial data set coupled with the urban population centers and infrastructure, allowed biometrics to begin to impact the counterinsurgency effort in a matter of months. In Afghanistan, the lack of an appreciable biometric collection, the difficult terrain, porous borders and sparse population centers significantly delayed the impact of biometrics.

Phase Zero collection as a strategy enhances homeland security in the short term by improving the biometric data available for screening suspected terrorists. In the long term, a Phase Zero strategy prepares the U.S. for potential conflicts around the globe. Through a DOTMLPF change recommendation, the DoD can develop the necessary policy and doctrine to enhance the military biometrics program. Though a National Security Presidential Directive mandating not only information sharing but coordinated collection activities and sharing agreements with other countries, the U.S. could maintain an advantage in the management of the identification. Through the targeted collection of biometrics in areas with strife and during humanitarian assistance missions as well as sharing information with partner nations on criminal files and international traveler biometrics, the database of valuable biometrics would grow rapidly. Only by embracing biometric as a key Phase Zero mission will the U.S. be prepared to leverage biometrics in the next counterinsurgency operation.

## BIBLIOGRAPHY

- al-Zawahiri, Ayman. "Letter in English." Office of the Director of National Intelligence. [http://www.dni.gov/press\\_releases/letter\\_in\\_english.pdf](http://www.dni.gov/press_releases/letter_in_english.pdf) (accessed October 17, 2011).
- Biometric Consortium. "Charter." (December 7, 1995), <http://www.biometrics.org/html/REPORTS/CTST96/> (accessed April 4, 2012).
- Biometrics Identity Management Agency (BIMA). "Biometrics Glossary." Version 5.0 (October 2010). <http://www.biometrics.dod.mil/Files/Documents/Standards/BioGlossary.pdf> (accessed February 2012).
- Biometrics Identity Management Agency (BIMA). *Biometrics Task Force Annual Report FY 08*. Biometrics Identity Management Agency. (Washington, D.C., 2009). <http://www.biometrics.dod.mil/Files/Documents/AnnualReports/fy08.pdf> (accessed February 11, 2012).
- Biometrics Identity Management Agency (BIMA). *BIMA Annual Report FY 10*. Biometrics Identity Management Agency. (Washington, D.C., 2011). <http://www.biometrics.dod.mil/Files/Documents/AnnualReports/fy10.pdf> (accessed February 11, 2012).
- Boyd, John. "Looking Back and Moving Forward...DoD Biometrics." Briefing, at the 2011 Biometric Consortium Conference, Tampa, FL, September 27, 2011.
- Bush, George W., "The New Way Forward in Iraq." (President's Address to the Nation, Washington, D.C., January 10, 2007). <http://georgewbush-whitehouse.archives.gov/news/releases/2007/01/20070110-7.html> (accessed February 11, 2012).
- "China and Korea boost biometrics at the border." *Biometric Technology Today* 2012, no. 1: 3. *Academic Search Premier*, EBSCOhost (accessed February 29, 2012).
- Computer Science Corporation. "Biometrics Identification System for Access." [http://assets1.csc.com/public\\_sector/downloads/0716\\_BISA\\_v6.pdf](http://assets1.csc.com/public_sector/downloads/0716_BISA_v6.pdf) (accessed February 9, 2012).
- Congressional Research Service Report for Congress. *Al Qaeda: Statements and Evolving Ideology (updated July 9, 2007)*. by Christopher M. Blanchard. <http://www.fas.org/sgp/crs/terror/RL32759.pdf> (accessed October 17, 2011).

- Congressional Research Service Report for Congress. *Presidential Directives: Background and Overview (updated April 23, 2007)*. by Harold C. Relyea. <http://www.fas.org/irp/crs/98-611.pdf> (accessed April 4, 2012).
- Cross Match Technologies. “Secure Electronic Enrollment Kit and Multimodal Identification Platform” [http://www.crossmatch.com/product\\_assets/brochures/SEEKII.pdf](http://www.crossmatch.com/product_assets/brochures/SEEKII.pdf) (accessed February 9, 2012).
- Daugman, John. “United Arab Emirates Deployment of Iris Recognition.” University of Cambridge. <http://www.cl.cam.ac.uk/~jgd1000/deployments.html> (accessed February 13, 2012).
- Etter, Dr. Delores M. “International Biometrics Report.” Report prepared for the Under Secretary of Defense for Policy, Southern Methodist University, Dallas TX, May 3, 2011, 3.
- Galula, David, and John A. Nagl. *Counterinsurgency Warfare: Theory and Practice*. Westport, CT: Praeger Security International, 2006.
- Johnson, Greg. “Biometrics Questions & Answers with Greg Johnson.” *Biometrics Bulletin* 2, no. 3 (May/June 2006). [http://www.biometrics.dod.mil/newsletter/issues/2006/may/v2issue3\\_a4htm](http://www.biometrics.dod.mil/newsletter/issues/2006/may/v2issue3_a4htm) (accessed November 2011).
- Kieffer, Jody and Kevin Trissell. “DOD Biometrics—Lifting the Veil of Insurgent Identity.” *Army AL&T* (April-June 2010). [http://asc.army.mil/docs/pubs/alt/2010/2\\_AprMayJun/articles/14\\_DOD\\_Biometrics--Lifting\\_the\\_Veil\\_of\\_Insurgent\\_Identity\\_201002.pdf](http://asc.army.mil/docs/pubs/alt/2010/2_AprMayJun/articles/14_DOD_Biometrics--Lifting_the_Veil_of_Insurgent_Identity_201002.pdf) (accessed February 11, 2012).
- Killion, Dr. Thomas. “National Defense Industrial Association Biometrics Conference Roadmap to Tomorrow.” Briefing, to the 2011 National Defense Industrial Association, Arlington, VA, February 23, 2012.
- Kitson, Frank. *Low Intensity Operations*. Hamden, Connecticut: Achon Books, 1974.
- Kroupa, Ken, Sr. “2010 Annual Biometrics Summit: Forensics enabling Biometrics.” Briefing at the 2010 Biometric Consortium Conference, Tampa, FL, September 22, 2010.
- L-1 Identity Solutions. “Portable Multimodal Enrollment and Recognition Device.” [http://www.l1id.com/files/224-HIIDE\\_0908\\_final.pdf](http://www.l1id.com/files/224-HIIDE_0908_final.pdf) (accessed February 9, 2012).



- Marighella, Carlos “Minimanual of the Urban Revolutionary Guerrilla,” in *Revolutionary Guerrilla Warfare*. Edited by Sam Sarkesian. Chicago: Precedent Publishing, Inc, 1975.
- Melshen, Paul. “Insurgency Theory ISC7” Lecture, Joint Forces Staff College, Norfolk, VA, September, 2011.
- McCuen, John J. *The Art of Counter-Revolutionary War: The Strategy of Counter-Insurgency*. Harrisburg, Pa.: Stackpole Books, 1966.
- Moss, Robert. “Urban Guerrilla Warfare,” in *Revolutionary Guerrilla Warfare*. Edited by Sam Sarkesian. Chicago: Precedent Publishing, Inc, 1975.
- Muller, Benjamin J. “Risking it all at the Biometric Border: Mobility, Limits, and the Persistence of Securitisation.” *Geopolitics* 16, no. 1 (2011): 91-106.  
<http://ezproxy6.ndu.edu/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=aph&AN=58528598&site=ehost-live&scope=site> (accessed February 29, 2012).
- National Science and Technology Council (NSTC). Subcommittee on Biometrics and Identity Management, “Biometrics History.” National Science and Technology Council. <http://www.biometrics.gov/Documents/BioHistory.pdf> (accessed February 11, 2012).
- National Science and Technology Council (NSTC). Subcommittee on Biometrics and Identity Management, “Biometrics Foundation Documents.” National Science and Technology Council. <http://www.biometrics.gov/documents/biofoundationdocs.pdf> (accessed February 26, 2012).
- Office of Management and Budget, Office of Information and Regulatory Affairs. *Defense Biometric Identification System (DBIDS): Attachment 3 Supplemental Information (History)*. Office of Management and Budget.  
[http://www.reginfo.gov/public/do/PRAViewIC?ref\\_nbr=200812-0704-003&icID=186430](http://www.reginfo.gov/public/do/PRAViewIC?ref_nbr=200812-0704-003&icID=186430) (accessed February, 11, 2012).
- . *Revolutionary Guerrilla Warfare*. Chicago: Precedent Pub., 1975.
- Seffers, George I. “U.S. Defense Department Expands Biometrics Technologies, Information Sharing.” *Signal* (October 2010).  
[http://www.afcea.org/signal/articles/templates/Signal\\_Article\\_Template.asp?articleid=2406&zoneid=285](http://www.afcea.org/signal/articles/templates/Signal_Article_Template.asp?articleid=2406&zoneid=285) (accessed February 11, 2012).
- Taber, Robert. *The War of the Flea: A Study of Guerrilla Warfare Theory and Practice*. New York: Lyle Stuart, 1965.

- Thompson, Robert. *Defeating Communist Insurgency*. London: Chatter and Windus, 1966.
- Trinquier, Roger. *Modern Warfare*. Westport, Connecticut: Praeger Security International, 2006.
- Tse-tung, Mao. *On Guerrilla Warfare*. Translated by Samuel B. Griffith II. Champaign, IL: University of Illinois Press, 2000.
- Tse-tung, Mao. *Selected Military Writings of Mao Tse-tung*. Peking: Foreign Languages Press, 1968.
- U.S. Department of Defense. *Department of Defense Biometrics*. DoD Directive 8521.01E. Washington D.C., February 21, 2008.
- U.S. Department of Defense. *DoD Personal Identity Protection (PIP) Program*. DoD Directive 1000.25. Washington D.C., April 25, 2007.
- U.S. Department of Defense. *Authority to Collect, Store, and Share Biometric Information of Non-U.S. Persons with U.S. Government Entities and Partner Nations*. Deputy Secretary of Defense Memorandum. Washington D.C., January 13, 2012.
- U.S. Department of Defense. *Sharing of Biometric Data and Associated Information from Non-U.S. Persons with Coalition Forces and Allies*. Deputy Secretary of Defense Memorandum. Washington D.C., January 10, 2007.
- U.S. Department of Defense. *Sharing of DoD Biometric Data and Associated UNCLASSIFIED Information from Non-U.S. Persons with Interagency Entities*. Deputy Secretary of Defense Memorandum. Washington D.C., January 10, 2007.
- U.S. Government Accounting Office. *Defense Biometrics: DOD Can Better Conform to Standards and Share Biometric Information with Federal Agencies*. Report, GAO-11-276. Washington D.C., March 2011.
- U.S. Joint Chiefs of Staff. *Operation of the Joint Capabilities Integration and Development System*. Chairman of the Joint Chiefs of Staff Manual 3170.01C. Joint Chiefs of Staff. Washington DC: May 1, 2007.
- U.S. Joint Chiefs of Staff. *Joint Intelligence*. Joint Publication 2-0. Joint Chiefs of Staff. Washington D.C.: June 22, 2007.
- U.S. Joint Chiefs of Staff. *Joint Operations*. Joint Publication 3-0. Joint Chiefs of Staff. Washington D.C.: August 11, 2011.

- U.S. Joint Chiefs of Staff. *Joint Urban Operations*. Joint Publication 3-06. Joint Chiefs of Staff. Washington D.C.: November 8, 2009.
- U.S. Joint Chiefs of Staff. *Stability Operations*. Joint Publication 3-07. Joint Chiefs of Staff. Washington D.C.: September 29, 2011.
- U.S. Joint Chiefs of Staff. *Antiterrorism*. Joint Publication 3-07.2. Joint Chiefs of Staff. Washington D.C.: November 24, 2010.
- U.S. Joint Chiefs of Staff. *Counterinsurgency Operations*. Joint Publication 3-24. Joint Chiefs of Staff. Washington D.C.: October 5, 2009.
- U.S. Joint Chiefs of Staff. *Command and Control for Joint Land Operations*. Joint Publication 3-31. Joint Chiefs of Staff. Washington D.C.: June 29, 2010.
- U.S. Joint Chiefs of Staff. *Joint Operations Planning*. Joint Publication 5-0. Joint Chiefs of Staff. Washington D.C.: August 11, 2011.
- U.S. Joint Chiefs of Staff. "Priorities for Biometrics in Support of Identity Management." Joint Staff Action Package J-8A 00077-11. Washington D.C., June 6, 2011.
- U.S. Joint Chiefs of Staff. "Stakeholder Priorities." Briefing, Biometrics Executive Committee, Washington D.C., June 23, 2011.
- U.S. Joint Forces Command. "Initial Capabilities Document (ICD): Biometrics in Support of Identity Management. Washington D.C., September 2, 2008.
- U.S. President, Homeland Security Presidential Directive/HSPD-11. "Comprehensive Terrorist-Related Screening Procedures." Public Papers of the Presidents of the United States: George W. Bush (2004, Book II), p. 1763 1765.  
<http://www.gpo.gov/fdsys/pkg/PPP-2004-book2/pdf/PPP-2004-book2-doc-pg1763.pdf> (accessed April 4, 2012).
- President, National Security Presidential Directive/NSPD-59 and Homeland Security Presidential Directive/HSPD-24. "Biometrics for Identification and Screening to Enhance National Security." Weekly Compilation of Presidential Documents Volume 44, Issue 22 (June 9, 2008). <http://www.gpo.gov/fdsys/pkg/WCPD-2008-06-09/pdf/WCPD-2008-06-09-Pg788-2.pdf> (accessed April 4, 2012).
- Whither Biometrics Committee. *Biometric Recognition: Challenges and Opportunities*. Edited by Joseph N. Pato and Lynette I. Millett. Washington, DC: National Academies Press, 2010.
- Woodward, John D., Nicholas Orlans and Peter T. Higgins. *Biometrics: Identity Assurance in the Information Age*. Emeryville, CA: McGraw-Hill, 2002.



## APPENDIX I: GENERAL HISTORY OF BIOMETRICS

Recall, biometrics is the joining of two words “bio” meaning life and “metrics” meaning to measure.<sup>1</sup> The application of this measurement of human life as an application to business and the military began long before the introduction of computers, but it was only through the advent of computers that the comparison of these measurements could be made on a large scale by those unfamiliar with the person or population being measured. The human brain registers patterns in appearance and modulations in speech and can recognize the identity of a person or persons previously encountered. This type of human-to-human recognition is largely unconscious.<sup>2</sup> When these persons are of the same socio-ethnic background the ability to differentiate between people improves over someone who is not from the same group or region. What the science of biometrics has done is reduce each person to a baseline set of measurements and it aides those unfamiliar with the person or the culture to distinguish one person from another. Through its link with forensics, it goes one-step further and allows for the identification of people not previously met. Some of the earliest demonstrations of what may be considered biometrics are in cave paintings.



<sup>1</sup> National Science and Technology Council (NSTC), Subcommittee on Biometrics and Identity Management, “Biometrics History,” National Science and Technology Council, <http://www.biometrics.gov/Documents/BioHistory.pdf> (accessed February 11, 2012).

<sup>2</sup> NSTC Biometrics History, <http://www.biometrics.gov/Documents/BioHistory.pdf> (accessed February 11, 2012).

More than 31,000 years ago prehistoric paintings included inked fingerprints which some believe may have served as an “unforgeable signature.”<sup>3</sup> Thousands of years later in 500 B.C., Babylonian business transaction recorded in clay included fingerprints.<sup>4</sup> In addition to using fingerprints as a means of signature, voice or more accurately modulation, was used in the Old Testament. The book of Judges chapter 12 in verses 5-6 addresses how the men of Gilead required suspected enemy soldiers to say the word “Shibboleth” when crossing the Jordan river. If spoken incorrectly the individual was deemed an Ephraimite and was slain.<sup>5</sup> The Bible records 42,000 Ephraimites were slain using this recognition pattern. Throughout time people have used biometrics to verify identities of individuals and distinguish friend from foe. Measurement of a person’s accent through listening or measurement a group’s tribe or region through visual observation of skin tone, facial features, and stature occurred daily. It was not until the 1800s with the Industrial revolution, when cities began to grow in size, that the need for a better means of identification was explored. As the population grew and mixed in demographics it was not possible to conduct business or govern by traditional methods and new methods were explored.<sup>6</sup> Largely two main approaches were developed. The first approach involved taking many physical measurements and recording these as a means of identifying the person later. The other involved the collection and classification of patterns found on the tips of the fingers.<sup>7</sup> Alphonse Bertillon developed the first approach in France in 1870. Bertillon referred to the process of detailed records of body

---

<sup>3</sup> NSTC Biometrics History, <http://www.biometrics.gov/Documents/BioHistory.pdf> (accessed February 11, 2012).

<sup>4</sup> Ibid.

<sup>5</sup> Judges 12: 5-6

<sup>6</sup> NSTC Biometrics History, <http://www.biometrics.gov/Documents/BioHistory.pdf> (accessed February 11, 2012).

<sup>7</sup> John D. Woodward, Nicholas Orlans and Peter T. Higgins, *Biometrics: Identity Assurance in the Information Age* (Emeryville, CA: McGraw-Hill, 2002), 26.

measurements including photographs and physical descriptions as “Bertillonage” which later came to be known as anthropometrics.<sup>8</sup> By systematically measuring and recording the dimensions of certain parts of the body, Bertillon found it possible to track repeat criminals even though they would change their names in an attempt to hide their identity. The second approach was to use the impressions left behind by a person’s finger or fingerprints. In 1892 Francis Galton published the book *Finger Prints*. In this seminal work, he stated that fingerprints had both individuality and permanence.<sup>9</sup> Consulting with Galton was Sir Edward Henry, the Inspector General of the Bengal Police in India. He was searching for a means of identification for criminals that could support or replace anthropometrics. In 1896 he developed a classification system for fingerprints, which would become the basis of the application of the science in London and serve as the precursor to the system used by the industrialized world, including the Federal Bureau of Investigation.<sup>10</sup> The two systems would finally come to a head in 1903 when the system developed by Bertillon demonstrated weakness. It is said that two men, later determined to be twins, were sentenced to jail in Leavenworth Kansas and were found to have nearly identical measurements. This event was used to challenge the claim that the Bertillon system could tell criminals apart.<sup>11</sup> Fingerprints became the recognized means of identification and anthropometrics as a means of identification faded into history.

---

<sup>8</sup> NSTC Biometrics History, <http://www.biometrics.gov/Documents/BioHistory.pdf> (accessed February 11, 2012).

<sup>9</sup> Woodward, *Biometrics*, 46.

<sup>10</sup> NSTC Biometrics History, <http://www.biometrics.gov/Documents/BioHistory.pdf> (accessed February 11, 2012).

<sup>11</sup> Ibid.

Biometric systems as recognized today did not develop until later in the twentieth century and were made possible by advances in computer technology.<sup>12</sup> Beginning in the late 1960s and 1970s many advances were made in semi-automated recognition of such biometrics as facial photos, voice, and fingerprints.<sup>13</sup> These advances were made within the academic community and were in support of pure science or at the behest of the United States government. The first commercially available application of biometric technology was as a means of physical access control. One of the earliest systems installed was an Identimat fingerprint-measurement device used as a time keeping and monitoring device for the Wall Street company Shearson Hamil. The focus on access control remained a key component of the early application of biometrics within the Department of Defense.

---

<sup>12</sup> NSTC Biometrics History, <http://www.biometrics.gov/Documents/BioHistory.pdf> (accessed February 11, 2012).

<sup>13</sup> Ibid.



## **APPENDIX II: KEY BIOMETRIC SYSTEMS**

There are, within the Department of Defense, key systems and biometric devices that make up the biometric enterprise. This section will not provide a complete discussion of those systems for two reasons. First, some systems and system linkages are beyond the scope of the classification of this paper. Second, it is not necessary to understand the entire biometrics enterprise to grasp the importance of biometrics to the counterinsurgency effort. By providing a brief description of the key systems used on the battlefield, the reader gains the understanding to follow the analysis later in the chapter.

### **Department of Defense Automated Biometric Identification System (DoD ABIS)**

According to the agency responsible for its administration, the Biometric Identity Management Agency (BIMA), “DoD ABIS is the central, authoritative, multi-modal biometric data repository.”<sup>14</sup> This means DoD ABIS is the central storage location for all red and non-United States citizen gray biometrics collected by the DoD. The database stores and matches the biometrics collected by the DoD and shares the data with other federal agencies such as the Federal Bureau of Investigations (FBI) and the Department of Homeland Security (DHS). The Integrated Automated Fingerprint Identification System (IAFIS) is the biometrics repository for the FBI and the Automated Biometric Identification System (IDENT) is the biometric repository for DHS.

---

<sup>14</sup> Biometrics Identity Management Agency (BIMA), “Biometrics Glossary,” Version 5.0 (October 2010), under “D,” <http://www.biometrics.dod.mil/Files/Documents/Standards/BioGlossary.pdf> (accessed February 9, 2012).

### **Biometric Automated Toolset (BAT)**

The Biometric Automated Toolset was the first system developed by the Department of Defense for the collection and matching of red and gray biometrics.

BIMA defines BAT as:

A multimodal biometric system that collects and compares fingerprints, iris images, and facial photos. It is used to enroll, identify and track persons of interest; build digital dossiers on the individuals that include interrogation reports, biographic information, relationships, etc.<sup>15</sup>

This may seem at odds with the definition of ABIS but the distinction is ABIS is the authoritative database and while the biometrics collected and stored in the BAT classified network are only a sub-set of the totality of the biometrics collected by DoD.

### **Biometric Identification System for Access (BISA)**

BIMA defines BISA as, “A biometric and contextual data collection and credential card production system.”<sup>16</sup> Within its function is a clearer explanation of the system. BISA is a system created to control access to United States installations in Iraq using a process involving biometric screening and the production of an access badge encoded with biometric information. In addition to the biometrically encoded badge, the BISA system captures biometrics and transmits them via satellite for comparison against both the ABIS and IAFIS databases. This process occurs in fairly short order.<sup>17</sup> More discussion will occur on the background for the development of BISA in the history section below.

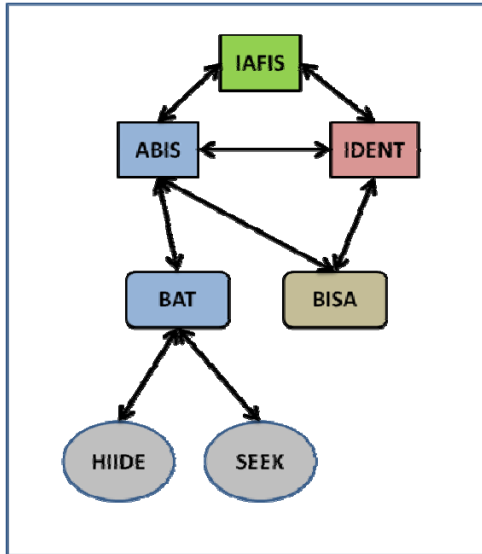
---

<sup>15</sup> Bimetrics Identity Management Agency (BIMA), “Biometrics Glossary,” Version 5.0 (October 2010), under “B,” <http://www.biometrics.dod.mil/Files/Documents/Standards/BioGlossary.pdf> (accessed February 9, 2012).

<sup>16</sup> Bimetrics Identity Management Agency (BIMA), “Biometrics Glossary,” Version 5.0 (October 2010), under “B,” <http://www.biometrics.dod.mil/Files/Documents/Standards/BioGlossary.pdf> (accessed February 9, 2012).

<sup>17</sup> Computer Science Corporation, “Biometrics Identification System for Access,” [http://assets1.csc.com/public\\_sector/downloads/0716\\_BISA\\_v6.pdf](http://assets1.csc.com/public_sector/downloads/0716_BISA_v6.pdf) (accessed February 9, 2012).

## Handheld Interagency Identity Detection Equipment (HIIDE)



The Handheld Interagency Identity Detection Equipment or HIIDE was the first handheld, mobile collection platform in wide use by United States conventional forces. The device collects fingerprints, iris images, facial photos, and contains a template for the collection of biographical information.<sup>18</sup> The HIIDE device attaches to the BAT to download collected biometrics for inclusion in DoD ABIS and to receive updates to biometric signatures included on

a watchlist.

## Secure Electronic Enrollment Kit II (SEEK II)

Like the HIIDE device, the SEEK II is a handheld biometric capture platform that must connect to a larger network to submit collected biometric signatures and receive updates on flagged biometrics. The device is multi-modal capturing fingerprints, iris images, and facial photos.<sup>19</sup> There are some distinct differences between the HIIDE and the SEEK II devices but these are not important to this thesis. What is germane is the fact that both are in use by conventional forces and represent the majority of the biometric enrollments populating the Department of Defense database.

<sup>18</sup> L-1 Identity Solutions, "Portable Multimodal Enrollment and Recognition Device," [http://www.l1id.com/files/224-HIIDE\\_0908\\_final.pdf](http://www.l1id.com/files/224-HIIDE_0908_final.pdf) (accessed February 9, 2012).

<sup>19</sup> Cross Match Technologies, "Secure Electronic Enrollment Kit and Multimodal Identification Platform," [http://www.crossmatch.com/product\\_assets/brochures/SEEKII.pdf](http://www.crossmatch.com/product_assets/brochures/SEEKII.pdf) (accessed February 9, 2012).

## **VITA**

Lt Col Green was commissioned in 1994 from the Air Force Reserve Officer Training Corps. Following initial training in Force Protection he served at numerous bases around the globe including South America, Iraq and Afghanistan. He has commanded Security Forces squadrons both stateside and deployed.

Lt Col Green is a graduate of the University of Maryland at College Park and has Master's degrees from George Washington University and the Defense Intelligence Agency. He is married to the former Sarah West and has four children.